

TeleWell VDSL2 switch User's Manual

***8-Port VDSL2 + 2 Gigabit TP/SFP
Layer 2 Managed Switch***

TABLE OF CONTENTS

1. INTRODUCTION	7
1.1 Package Contents	7
1.2 Product Description	8
1.3 How to Use This Manual	9
1.4 Product Features	10
1.5 Product Specification	12
2. INSTALLATION.....	15
2.1 Hardware Description	15
2.1.1 Switch Front Panel	15
2.1.2 LED Indications.....	17
2.1.3 Switch Rear Panel	20
2.2 Install the Switch.....	22
2.2.1 Desktop Installation	22
2.2.2 Rack Mounting.....	23
2.2.3 Installing the SFP transceiver.....	25
2.3 Wiring for VDSL2 Ports	27
3. SWITCH MANAGEMENT	30
3.1 Requirements	30
3.2 Management Access Overview	31
3.3 Web Management.....	32
3.4 SNMP-Based Network Management	33
3.5 Administration Console.....	33
3.6 Protocols.....	35
3.6.1 Virtual Terminal Protocols	35
3.6.2 SNMP Protocol	35
3.6.3 Management Architecture	35
4. WEB-BASED MANAGEMENT	36
4.1 About Web-based Management	36
4.1.1 Requirements	37
4.1.2 Logging on the switch.....	37
4.1.3 Main WEB PAGE.....	39
4.2 System.....	40
4.2.1 System Information.....	41

4.2.2 IP Configuration	45
4.2.3 Console Port Info	47
4.2.4 SNMP Configuration	47
4.2.5 Syslog Setting	54
4.2.6 Firmware Upgrade	55
4.2.7 Configuration Backup	57
4.2.8 Factory Default	60
4.2.9 System Reboot	60
4.3 Port Configuration	61
4.3.1 Port Control	61
4.3.2 Port Status	63
4.3.3 Port Statistics	63
4.3.4 Port Sniffer	64
4.3.5 Protect Port	66
4.4 VLAN configuration	67
4.4.1 VLAN Overview	67
4.4.2 Static VLAN Configuration	70
4.4.3 Port-based VLAN	71
4.4.4 802.1Q VLAN	73
4.4.5 Q-in-Q VLAN	78
4.4.6 GVRP VLAN	82
4.5 Trunking	85
4.5.1 Aggregator setting	85
4.5.2 Aggregator Information	86
4.5.3 State Activity	90
4.6 Forwarding and Filtering	91
4.6.1 Dynamic MAC Table	91
4.6.2 Static MAC Table	92
4.6.3 MAC Filtering	93
4.7 IGMP Snooping	94
4.7.1 Theory	94
4.7.2 IGMP Configuration	98
4.8 Spanning Tree Protocol	99
4.8.1 Theory	99
4.8.2 Illustration of STP	102
4.8.3 STP Parameters	103

4.8.4 STP System Configuration	105
4.8.5 Port Configuration	108
4.9 DHCP Relay & Option 82	110
4.10 LLDP	112
4.10.1 LLDP Configuration	112
4.10.2 PerPort Configuration	113
4.11 Access Control List	114
4.12 Security Manager	118
4.13 MAC Limit	118
4.13.1 MAC Limit Configuration.....	118
4.13.2 MAC Limit Port Status	119
4.14 802.1x Configuration.....	120
4.14.1 Understanding IEEE 802.1x Port-Based Authentication	120
4.14.2 System Configuration	123
4.14.3 802.1x PerPort Configuration	125
4.14.4 Misc Configuration	126
4.15 QoS Configuration	127
4.15.1 Understand QoS	127
4.15.2 QoS Configuration	128
4.15.3 TOS/DSCP	131
4.16 VDSL Configuration	134
4.16.1 Profile Configuration	134
4.16.2 VDSL Port Status	138
5. CONSOLE MANAGEMENT	142
5.1 Login in the Console Interface	142
5.2 Configure IP address	143
5.3 Commands Level	145
6. COMMAND LINE INTERFACE	146
6.1 Operation Notice	146
6.2 System Commands.....	147
6.3 Switch Static Configuration	148
6.3.1 Port Configuration and show status	148
6.4 Trunk Configuration.....	152
6.4.1 Trunking Commands	152
6.4.2 LACP Command.....	153
6.5 VLAN Configuration.....	155

6.5.1 Virtual LANs.....	155
6.5.2 VLAN Mode: Port-based.....	156
6.5.3 Advanced 802.1Q VLAN Configuration.....	157
6.6 Misc Configuration.....	160
6.7 Administration Configuration.....	161
6.7.1 Change Username / Password.....	161
6.7.2 IP Configuration.....	162
6.7.3 Reboot switch.....	163
6.7.4 Reset to Default.....	163
6.7.5 TFTP Update Firmware.....	163
6.7.6 Restore Configuration File.....	163
6.7.7 Backup Configuration File.....	164
6.8 MAC limit.....	164
6.9 Port Mirroring Configuration.....	165
6.10 Quality of Service.....	166
6.10.1 QoS Configuration.....	166
6.10.2 Per-Port Priority.....	167
6.11 MAC Address Configuration.....	168
6.12 STP/MSTP Commands.....	170
6.13 SNMP.....	177
6.13.1 System Options.....	177
6.13.2 Community Strings.....	178
6.13.3 Trap Managers.....	178
6.14 IGMP.....	179
6.15 802.1x Protocol.....	181
6.16 Access Control List.....	184
6.16.1 IPv4 ACL commands.....	184
6.16.2 Non-IPv4 ACL commands.....	186
6.17 Binding.....	187
6.17.1 SIP/SMAC binding commands.....	187
6.18 VDSL2 Commands.....	189
6.18.1 VDSL2 interface Commands.....	189
6.18.2 VDSL2 profile Commands.....	192
7. SWITCH OPERATION.....	202
7.1 Address Table.....	202
7.2 Learning.....	202

7.3 Forwarding & Filtering 202

7.4 Store-and-Forward 202

7.5 Auto-Negotiation 202

8. TROUBLESHOOTING..... 204

APPENDIX A—RJ-45/-21 PIN ASSIGNMENT 206

 A.1 Switch's RJ-45 Pin Assignments 206

 A.2 10/100Mbps, 10/100Base-TX..... 206

 A.3 RJ-21 (Telco-50) Connector pin-out for VCO-24..... 208

 A.4 RJ-21 (Telco 50) Cable pin-out..... 209

1. INTRODUCTION

The Layer 2 Managed Switch series are multiple VDSL2 ports Ethernet Switched with Gigabit TP/SFP fiber optical combo connective ability and robust layer 2 features; the description of these modelsⁱ as below:

VCO-8 :	8-Port VDSL2 + 2-Port Gigabit TP/SFP Combo Managed Switch
VCO-24 AC :	24-Port VDSL2 + 2-Port Gigabit TP/SFP Combo Managed Switch / AC Power
VCO-24D C :	24-Port VDSL2 + 2-Port Gigabit TP/SFP Combo Managed Switch / DC Power



VCO-8



VCO-24AC / VCO-24DC

Terms of “**Managed Switch**” means the Switches mentioned titled in the cover page of this User's manual.

1.1 Package Contents

Open the box of the Managed Switch and carefully unpack it. The box should contain the following items:

Check the contents of your package for following parts:

☒ The Managed Switch	x1
☒ User's Manual CD	x1
☒ Quick Installation Guide	x1
☒ 19" Rack mount Accessory Kit	x1
☒ Power Cord	x1
☒ Rubber Feet	x4
☒ RS-232 DB9 female Console Cable	x1
☒ 2 meter Telco-50 Cable (VCO-24ⁱⁱ Only)	x1

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the carton including the original packing material, and use them against to repack the product in case there is a need to return it to us for repair.

ⁱ The model names (VCO-8, VCO-24AC and VCO-24DC) might not be actual model names.

ⁱⁱ VCO-24 stands for either VCO-24AC and/or VCO-24DC.

1.2 Product Description

Overview

The VCO-8 and VCO-24 are Ethernet over VDSL2 switches with multiple VDSL2 ports and two Gigabit TP/SFP combo interfaces on the front panel high-speed uplink or long distance fiber optical link. The Switch is a DSLAM (Digital Subscriber Line Access Multiplexer) accommodating well proven Ethernet and VDSL2 technologies to extend Ethernet over single-pair phone line by using a VDSL2 signal.

High Performance over Telephone Line

Up to **100/100Mbps** bandwidth less than 1000ft provides ultra-high performance to the pervasive telephone line network, and has the advantage of minimum installation time and minimum expense by allowing voice and data to share the same telephone pair without interference. Moreover, the maximum 1.4km distance provides wide coverage for service providers.

Friendly / Simple Web Management Interface

The VDSL2 Switch contains an advanced management capability that can be remotely accessed by Web Browser and SNMP. The standard IEEE 802.1Q with VLAN tagging feature makes logically separating nodes easier with up to 256 VLAN groups allowed. Four priority queues with 802.1p support, IGMP snooping and rate control function are also provided to optimize network bandwidth. Additionally, its standard-compliant implementation ensures interoperability with equipment from other vendors.

Long Distance / High Performance backbone Extend

The two Gigabit TP/SFP combo interface provides fat pipes for connecting to the backbone or connecting to servers. 10/100/1000Base-T, 1000Base-SX and 1000Base-LX modules are available to fit existing networks and to provide flexible media selections. The mini-GBIC slots 1000Base-SX/LX through SFP (Small Form-factor Pluggable) interface. The distance can be extended from 100 meters (TP), 550 meters (Multi-mode fiber), up to above **10/30/50/70/120 kilometers** (Single-mode fiber).

Cost-effective solution with SNMP monitor for Network deployment

Not only for catering to the need of easy WEB-based management but also the centralized SNMP application to monitor the status of Switch and traffic per port. The key features are as below:

- **WEB / SSL / Telnet / Console management**
- **802.1Q / Q-in-Q VLAN**
- **Rapid Spanning Tree**
- **IGMP Snooping**
- **802.1x Authentication / RADIUS**
- **Access Control List**
- **SNMP and 4 RMON groups**

Powerful Security

The VDSL2 Managed Switch offers comprehensive Access Control List (ACL) for enforcing security to the edge. Its protection mechanisms comprises of Port-based 802.1x user and device authentication. Moreover, the switch provides MAC filter and Static MAC for enforcing security policies to the edge. The administrators can now construct highly secured corporate networks with considerably less time and effort than before.

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, INSTALLATION

The section explains the functions of the Switch and how to physically install the Managed Switch.

Section 3, SWITCH MANAGEMENT

The section contains the information about the software function of the Managed Switch.

Section 4, WEB-BASED MANAGEMENT

The section explains how to manage the Managed Switch by Web interface.

Section 5, CONSOLE MANAGEMENT

The section describes how to use the Console management interface.

Section 6, COMMAND LINE INTERFACE

The section explains how to manage the Managed Switch by Command Line interface.

Section 7, SWITCH OPERATION

The chapter explains how to do the switch operation of the Managed Switch.

Section 8, TROUBLESHOOTING

The chapter explains how to trouble shooting of the Managed Switch.

Appendix A, RJ-45/RJ-21 PIN ASSIGNMENT

The section contains connector pin information of the Managed Switch.

1.4 Product Features

➤ VDSL Interface

VCO-24 AC / VCO-24DC

- 24 VDSL2 links via **RJ-21 (Telco-50)** connector
- 24 corresponding POTS lines via **RJ-21 (Telco-50)** connector
- Built-in **POTS splitter** for each VDSL port
- Auto-speed function for VDSL2 link (by distance and cable quality)

VCO-8

- 8 x **RJ-11** connectors for VDSL2 connection
- 8 x **RJ-11** connectors for telephone/POTS connection
- Built-in **POTS splitter** for each VDSL port
- Auto-speed function for VDSL2 link (by distance and cable quality)

➤ Ethernet Interface

- 2 10/100/1000Mbps TP and SFP shared combo interfaces
- Auto-MDI/MDI-X detection on Gigabit **RJ-45** port

➤ VDSL2 Features

- Cost-effective VDSL2 link and central management solution
- ITU-T G.993.2 VDSL2 standard
- DMT (Discrete Multi-Tone) line coding VDSL
- Selectable bandwidth control and target SNR margin
- Built-in surge protection to against surge damage from high energy spike
- Voice and data communication can be shared on the existing telephone wire simultaneously

➤ Layer 2 Features

- Prevents packet loss Flow Control:
 - IEEE 802.3x PAUSE frame Flow Control for Full-Duplex mode
 - Back-Pressure Flow Control in Half-Duplex mode
- High performance Store and Forward architecture, broadcast storm control, runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
- 8K MAC Address Table, automatic source address learning and ageing
- Support **VLAN**:
 - IEEE 802.1Q Tag-Based VLAN
 - Port-Based VLAN
 - Q-in-Q tunneling (Double Tag VLAN)
 - GVRP for dynamic VLAN Management
 - Private VLAN Edge (PVE / Protected Port)
- Supports **Link Aggregation**
 - Up to 13 Trunk groups
 - Up to 8 ports per trunk group with 1.6Gbps bandwidth (Full Duplex mode)
 - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
 - Cisco ether-Channel (Static Trunk)
- Support **Spanning Tree Protocol**:

- STP, IEEE 802.1D (Classic Spanning Tree Protocol)
- MSTP, IEEE 802.1s (Multiple Spanning Tree Protocol, spanning tree by VLAN)

➤ **Quality of Service**

- 4 priority queues on all switch ports
- Traffic classification:
 - IEEE 802.1p Class of Service
 - IP TOS / DSCP code priority
 - Port Base priority
- Strict priority and weighted round robin (WRR) CoS policies
- Ingress/Egress Bandwidth control on each port

➤ **Multicast**

- IGMP Snooping v1 and v2
- IGMP Snooping v2 fast leave
- IGMP Query mode for Multicast Media application

➤ **Security**

- IEEE 802.1x Port-Based network access control protocol
- RADIUS users access authentication
- L3 / L4 Access Control List (ACL)
- Source IP-MAC / Port-Binding
- Port Security for Source MAC address entries filtering

➤ **Management**

- Switch Management Interface
 - Telnet Command Line Interface
 - Web-based switch management
 - SNMP v1, v2c, v3 switch management
 - SSL switch management
- DHCP client for IP address assignment
- DHCP Option82 and DHCP Relay
- Link Layer Discovery Protocol (LLDP) for easy network management
- Built-in Trivial File Transfer Protocol (TFTP) client
- Firmware upgrade via TFTP or HTTP
- Configuration restore / backup via TFTP or HTTP
- Event message logging to remote Syslog server
- Four RMON groups 1, 2, 3, and 9 (history, statistics, alarms, and events)
- SNMP trap for interface Link Up and Link Down notification
- Supports Ping function
- Reset button for system reboot or reset to factory default
- 1 RS-232 male DB9 console interface for Switch basic management and setup

1.5 Product Specification

Product	VCO-8	VCO-24AC	VCO-24DC
Hardware Specification			
VDSL2 Interface	8-Port VDSL2 RJ-11 connector	24-Port VDSL2 RJ-21(Telco-50) connector	
	8-Port POTS/Telephone RJ-11 connector	24-Port POTS/Telephone RJ-21(Telco-50) connector	
	1000Mbps Copper Ports 2 10/100/1000Mbps RJ-45 Auto-MDI/MDI-X ports		
SFP/mini-GBIC Slots	2 1000Base-SX/LX/BX, shared with Port-9~Port-10	2 1000Base-SX/LX/BX, shared with Port-25~Port-26	
Surge protect	3KV	3KV	
Console	1 x RS-232 Serial Port (DB9, 57600, 8, N, 1)		
Switch Architecture	Store-and-Forward		
Switch Fabric	5.6Gbps / non-blocking	8.8Gbps / non-blocking	
Switch Throughput	4.16Mpps @64Bytes	6.547Mpps @64Bytes	
Address Table	8K entries		
Share Data Buffer	256K Bytes	512K Bytes	
Maximum Frame Size	9K Bytes packet		
Flow Control	Back pressure for Half Duplex IEEE 802.3x Pause Frame for Full Duplex		
LED	System: Power Status Alert: FAN 1, FAN2, FAN3 VDSL: VDSL Link/Sync. Gigabit Port: 1000 Link/Active, 100 Link/Active	System: Power, Status Alert: FAN 1, FAN 2, Power 1, Power 2 VDSL: VDSL Link/Sync. Gigabit Port: 1000 Link/Active, 100 Link/Active	
Reset Button	< 5 seconds: System reboot > 5 seconds: Factory Default		
Dimension (W x D x H)	440 x 220 x 44mm 1U height	440 x 351 x 88mm 2U height	
Weight	2.9kg	6.4kg - with one AC Power module	6.4kg - with one DC Power module
Power Requirement	100~240V AC, 50/60Hz	100~240V AC, 50/60Hz	48V DC (Range: 30V~60V)
Power Consumption	System ON: 26.7 Watts max. Full Load: 57.2 Watts max.	System ON: 73.5 Watts max. Full Load: 117 Watts max.	
Cables	◦ VDSL: twisted-pair telephone wires (AWG24 or better) up to 1.4km ◦ 10Base-T: 2-Pair UTP Cat.3,4,5 up to 100m (328ft) ◦ 100Base-TX: 2-Pair UTP Cat.5, up to 100m (328ft) ◦ 1000Base-T: 4-pair UTP Cat 5E, up to 100m		

	1000Base-SX: 50/125µm and 62.5/125µm fiber-optic cable, up to 550m 1000Base-LX: 9/125µm fiber optic cable, from 10km to 120km
VDSL2	
VDSL2 Standard	Comply with ITU-T G.993.1 and G.993.2. Supports provisioning the VDSL optional band (25K to 138K Hz) usage
Band Plan	Selectable band plan for each VDSL line on a per port basis Band plan A: - Profile 998, Annex A of G.993.1 Band plan B: - Profile 997, Annex B of G.993.1
Profile	Selectable spectrum profile of 8a/b/c/d, 12a/b, 17a, and 30a for frequency bands (Annex A, B and C) defined in G.993.2
Encoding	VDSL-DMT
VDSL2 Features	Selectable rate limit control Selectable target SNR (Signal to Noise Ratio) mode POTS voices pass through
Layer 2 Function	
Management Interface	Console, Telnet, Web Browser, SSL, SNMPv1/v2c/v3
Gigabit Port Configuration	Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow Control disable / enable
Gigabit Port Status	Display each port's speed duplex mode, link status and Flow control status. Auto negotiation status, trunk status.
Port Mirroring	TX / RX / Both 1 to 1 monitor
Bandwidth Control	Ingress / Egress rate limit control Gigabit Port: - Allow to configure per 128Kbps VDSL2 Port: - Allow to configure per 5Mbps
VLAN	IEEE 802.1Q Tag-based VLAN, up to 255 VLANs groups, out of 4041 VLAN IDs Port-based VLAN GVRP Q-in-Q tunneling Private VLAN Edge(PVE / Protected port) with two protected port groups
Link Aggregation	Static Port Trunk IEEE 802.3ad LACP (Link Aggregation Control Protocol) Supports 13 groups of 8-Port trunk support
QoS	4 priority queue Traffic classification based on: - Port priority 802.1p priority - DSCP/TOS field in IP Packet
IGMP Snooping	IGMP (v1/v2) Snooping, up to 256 multicast Groups
Access Control List	IP-Based Layer 3 / Layer 4 ACL Up to 220 ACL rule entries

SNMP MIBs	RFC-1213 MIB-II RFC-2863 Interface MIB RFC-2665 EtherLike MIB RFC-1493 Bridge MIB RFC-2819 RMON MIB (Group 1, 2, 3 and 9) RFC-2737 Entity MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Protocols and Standards Compliance	ITU-T - G.993.1 (VDSL) - G.997.1 - G.993.2 VDSL2 IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab 1000BASE-T IEEE 802.3x Flow Control IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.1d Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2

2. INSTALLATION

This section describes the hardware features and installation of the Managed Switch on the desktop or rack mount. For easier management and control of the Managed Switch, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Managed Switch, please read this chapter completely.

2.1 Hardware Description

2.1.1 Switch Front Panel

The unit front panel provides a simple interface monitoring the switch. [Figure 2-1-1 to 2-1-2](#) shows the front panel of the Managed Switches.

VCO-24 Front Panel

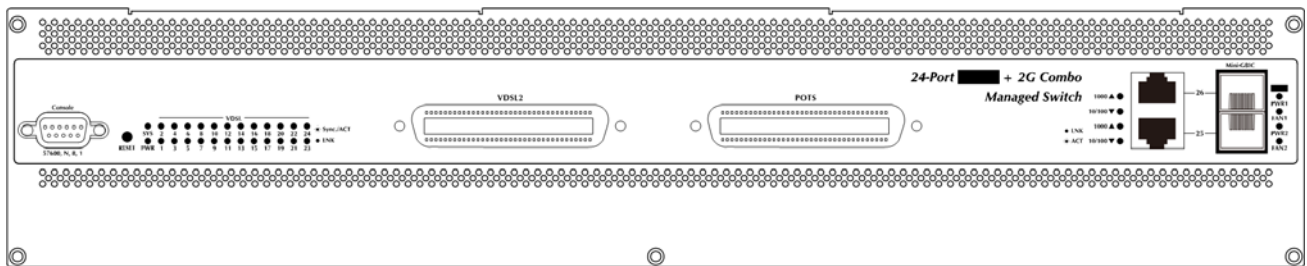


Figure 2-1-1: VCO-24 front panel

VCO-8 Front Panel

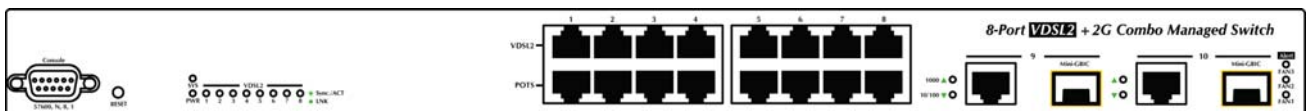


Figure 2-1-2: VCO-8 front panel

■ Console Port

The console port is a DB9, RS-232 male serial port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information includes IP Address setting, factory reset, port management, link status and system setting. Users can use the attached RS-232 cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm, and so on) to enter the startup screen of the device.

■ VDSL2 and POTS interface

There are 24 VDSL2 ports and 24 POTS ports with 2 RJ-21 (Telco-50) type connectors on the front panel of VCO-24 and there are 8 VDSL2 ports and 8 POTS ports with RJ-11 phone connectors on the front panel of VCO-8. Each port is built-in POTS splitter that helps the voice of telephone and data of network applications transmitting at the same wire without interrupted.

The VDSL2 supports auto detection transmission rate that operate in different band allocation and result in different upstream and downstream bandwidth. And due to different telephone line quality, cross talk or extension distance may affect actual achievable speed; you can configure individual port in built-in management interface for optimized connectivity.



1. The payload rate is about 9% less than the line rate due to framing overhead.
2. AWG26 (0.4mm) cable can also be used but the distance is 20% to 40% shorter than AWG24 cable.
3. Each terminated bridge tap can reduce the VDSL link distance by 90m. The quality of the cable, the size of the cable bundles, and the cross talk within the bundle, can also affect other overall reach.

■ Gigabit TP Interface

VCO-24: Port-25 and Port-26

VCO-8: Port-9, Port-10

10/100/1000Base-T Copper, RJ-45 Twisted-Pair: Up to 100 meters.

■ Gigabit SFP Slots

VCO-24: Port-25 and Port-26

VCO-8: Port-9, Port-10

1000Base-SX/LX mini-GBIC slot, SFP (Small Form-factor Pluggable) transceiver module: From 550 meters (Multi-mode fiber), up to 10/30/50/70/120 kilometers (Single-mode fiber).

■ Reset button

At the left of front panel, the reset button is designed for reboot the Managed Switch without turn off and on the power.

The following is the summary table of Reset button functions:

Reset Button Pressed and Released	Function
About 1~5 seconds	Reboot the Managed Switch
Until the SYS LED lit off	Reset the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings as below: ◦ Default Username/Password: admin/admin ◦ Default IP address: 192.168.0.100 ◦ Subnet mask: 255.255.255.0 ◦ Default Gateway: 192.168.0.254

2.1.2 LED Indications

The front panel LEDs indicate instant status of port links, data activity and system power; helps monitor and troubleshoot when needed.

VCO-24 LED indication

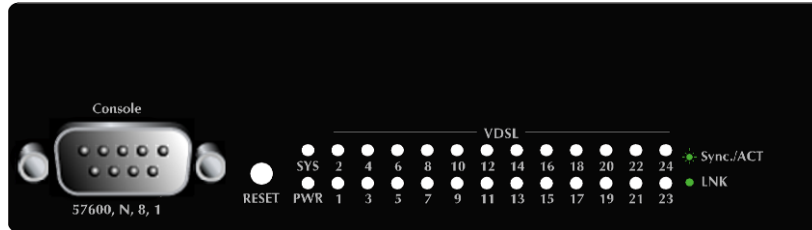


Figure 2-1-3: VCO-24 System and Port LED panel

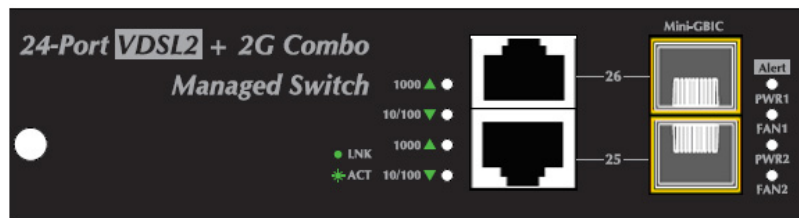


Figure 2-1-4: VCO-24 Power and Fan LED panel

■ System

LED	Color	Function	
PWR	Green	On:	Indicate that the Switch is powered on
		Off:	Indicate that the Switch is powered off
SYS	Orange	Lit:	Lights to indicate the system is working.
		Blink:	Indicate that the system is in OS boot procedure or reset to default
PWR1	Orange	On:	Indicate that power1 is inserted and failed to work.
FAN1	Orange	On:	Indicate that fan1 is failed to work.
PWR2	Orange	On:	Indicate that power2 is inserted and failed to work.
FAN2	Orange	On:	Indicate that fan2 is failed to work.

■ Per VDSL Interface (Port-1 to Port-24)

LED	Color	Function	
VDSL LNK/Sync	Green	On:	Indicate that the VDSL link is established.
		Slow Blink:	Indicate that the VDSL is at training status with remote CPE
		Quick Blink:	Indicate that the DATA link is actively sending or receiving data over that VDSL port
		Off:	Indicate that the VDSL is link down

■ 10/100/1000Base-T Copper / 1000Base-SX/LX SFP Interface (Port-25 and Port-26)

LED	Color	Function	
1000 LNK/ACT	Green	On:	To indicate the link through that port is successfully established with speed 1000Mbps
		Blink:	To indicate that the switch is actively sending or receiving data over that port.
		Off:	If 10/100 LNK/ACT LED is light, it indicates that the port is operating at 10Mbps or 100Mbps If LNK/ACT LED is Off, it indicates that the port is link down
10/100 LNK/ACT	Green	On:	To indicate the link through that port is successfully established with speed 10Mbps or 100Mbps
		Blink:	To indicate that the switch is actively sending or receiving data over that port.
		Off:	If 1000 LNK/ACT LED is light, indicates that the port is operating at 1000Mbps If 1000 LNK/ACT LED is Off, it indicates that the port is link down

VCO-8 LED indication

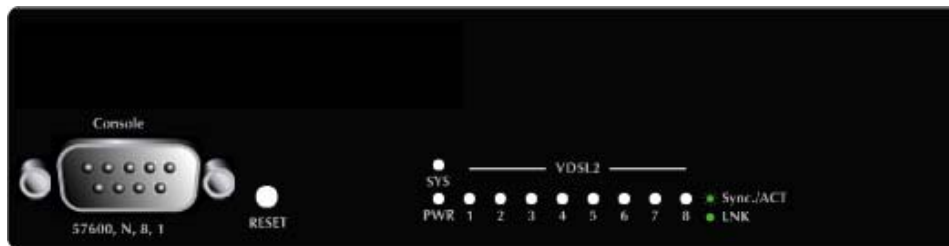


Figure 2-1-5: VCO-8 System and Port LED panel



Figure 2-1-6: VCO-8 Fan Alert LED panel

■ System

LED	Color	Function	
PWR	Green	On:	Indicate that the Switch is powered on
		Off:	Indicate that the Switch is powered off
SYS	Orange	On:	Lights to indicate the system is working.
		Blink:	Indicate that the system is in OS boot procedure or reset to default

FAN1 Alert	Orange	On:	Lights to indicate that the FAN1 failure
FAN2 Alert	Orange	On:	Lights to indicate that the FAN2 failure
FAN3 Alert	Orange	On:	Lights to indicate that the FAN3 failure

■ Per VDSL Interface (Port-1 to Port-8)

LED	Color	Function	
VDSL LNK/Sync	Green	On:	Indicate that the VDSL link is established
		Slow Blink:	Indicate that the VDSL is at training status with remote CPE
		Quick Blink:	Indicate that the DATA link is actively sending or receiving data over that VDSL port
		Off:	Indicate that the VDSL is link down

■ 10/100/1000Base-T Copper / 1000Base-SX/LX SFP Interface (Port-9 and Port-10)

LED	Color	Function	
1000 LNK/ACT	Green	On:	To indicate the link through that port is successfully established with speed 1000Mbps
		Blink:	To indicate that the switch is actively sending or receiving data over that port.
		Off:	If 10/100 LNK/ACT LED is light, it indicates that the port is operating at 10Mbps or 100Mbps If LNK/ACT LED is Off, it indicates that the port is link down
10/100 LNK/ACT	Green	On:	To indicate the link through that port is successfully established with speed 10Mbps or 100Mbps
		Blink:	To indicate that the switch is actively sending or receiving data over that port.
		Off:	If 1000 LNK/ACT LED is light, it indicates that the port is operating at 1000Mbps If 1000 LNK/ACT LED is Off, it indicates that the port is link down



The 2 Gigabit TP/SFP combo ports are shared with Port 9/10 of VCO-8 or Port25/26 of VCO-24. Either of them can operate at the same time.

2.1.3 Switch Rear Panel

The VCO-24AC equip with one 100~240V AC power supply unit and VCO-24DC equip with one DC -48V power supply unit on its standard package, both VCO-24AC and VCO-24DC provide one spare power supply unit slot for option redundant power supply installation. A redundant power supply is also provided to enhance the reliability with options of either 100~240V AC power supply unit or DC -48V power supply unit.

VCO-24 AC Rear Panel

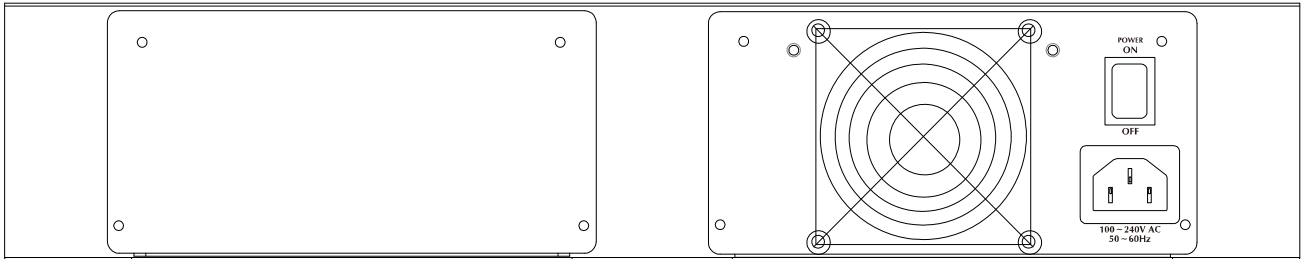


Figure 2-1-7: VCO-24AC rear panel with AC power module

VCO-24DC Rear Panel

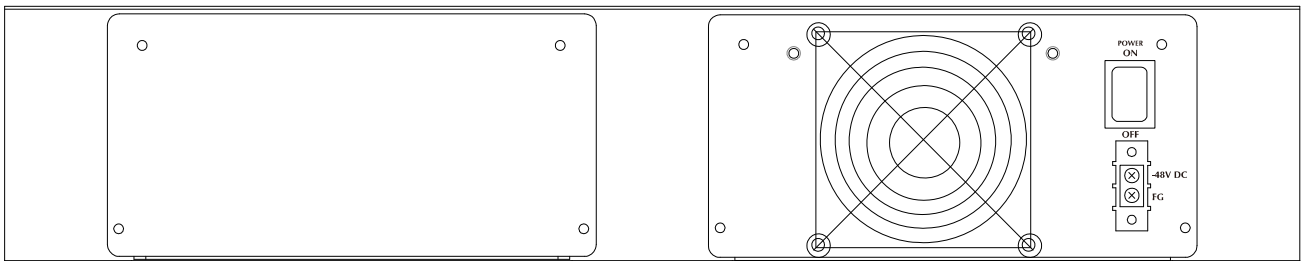


Figure 2-1-8: VCO-24DC rear panel with DC power module

Install and remove the power supply unit

To install a power supply unit to VCO-24 box, please fasten the hand screw clockwise and slide in the power supply unit to the Managed Switch.

To remove a power supply unit out the VCO-24, please loose the hand screw counter clockwise and pull out the power supply unit from the VCO-24 box.



Figure 2-1-9: Install and remove the power supply unit of VCO-24 box

The rear panel of VCO-8 indicates an AC inlet power socket, which accepts input power from 100 to 240V AC, 50-60Hz.

Figure 2-1-10 shows the rear panel of the Managed Switch.

VCO-8 Rear Panel



Figure 2-1-10: VCO-8 rear panel

-
1. The device is a power-required device, it means, it will not work till it is powered. If your networks should active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.

Power Notice:

2. In some area, installing a surge suppression device may also help to protect your Managed Switch from being damaged by unregulated surge or current to the Switch or the power adapter.
-

2.2 Install the Switch

This section describes how to install the Managed Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.2.1 Desktop Installation

To install the Managed Switch on desktop or shelf, please follows these steps:

Step1: Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

Step2: Place the Managed Switch on the desktop or the shelf near an AC power source.

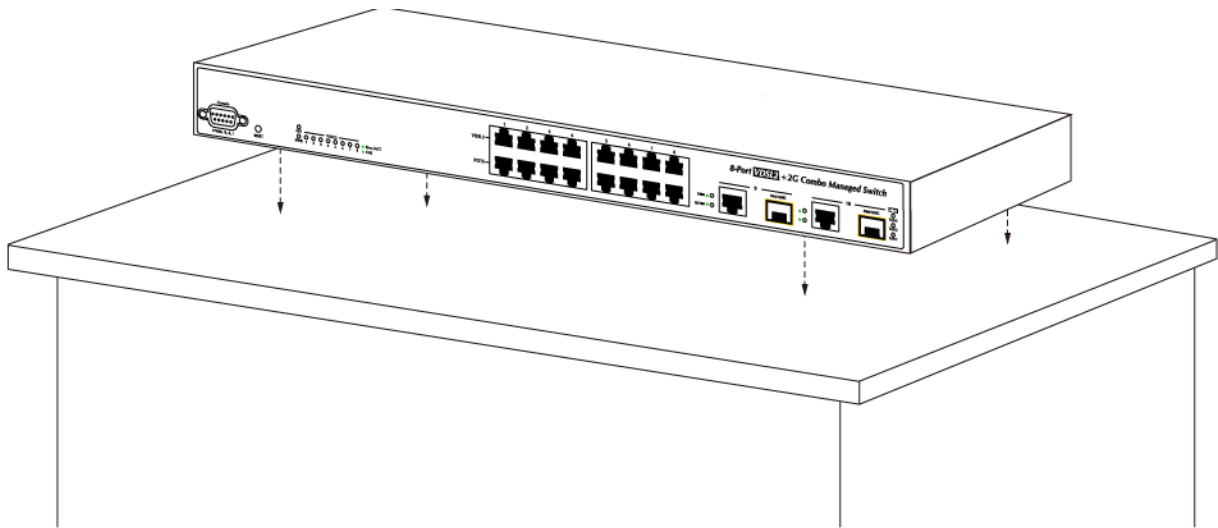


Figure 2-2-1: Place the Managed Switch on the desktop

Step3: Keep enough ventilation space between the Managed Switch and the surrounding objects.



When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4, in Specification.

Step4: Connect the Managed Switch to network devices.

- A. Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the Managed Switch
- B. Connect the other end of the cable to the network devices such as printer servers, workstations or routers...etc.



Connection to the Managed Switch requires UTP Category 5 (5E is better) network cabling with RJ-45 tips. For more information, please see the Cabling Specification in Appendix A.

Step5: Supply power to the Managed Switch.

- A. Connect one end of the power cable to the Managed Switch.
- B. Connect the power plug of the power cable to a standard wall outlet.

When the Managed Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the Managed Switch in a 19-inch standard rack, please follow the instructions described below.

Step1: Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

Step2: Attach the rack-mount bracket to each side of the Managed Switch with supplied screws attached to the package.

Figure 2-2-2 and Figure 2-2-3 shows how to attach brackets to one side of the Managed Switch.

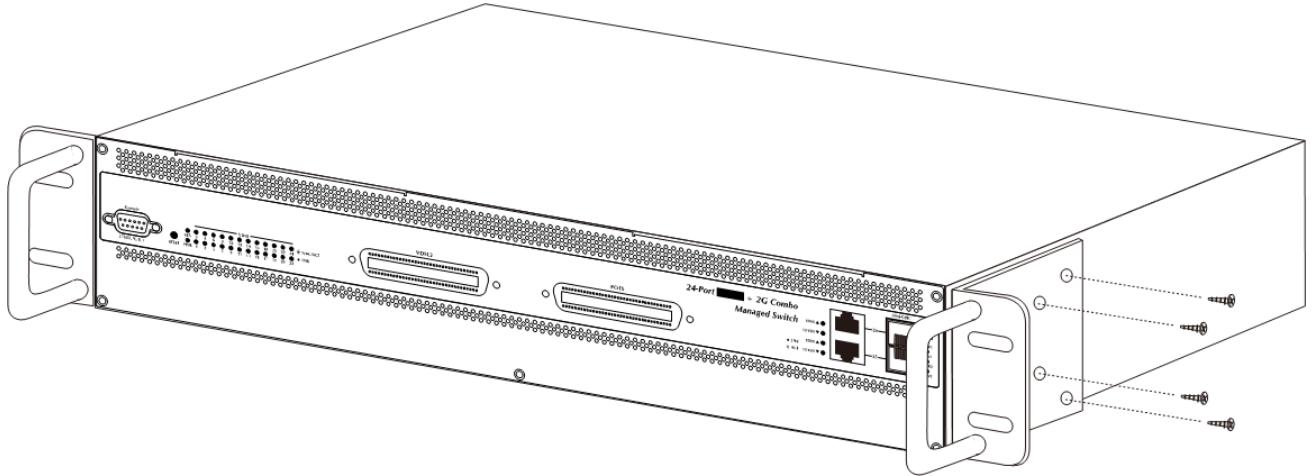


Figure 2-2-2: Attach brackets to VCO-24 series

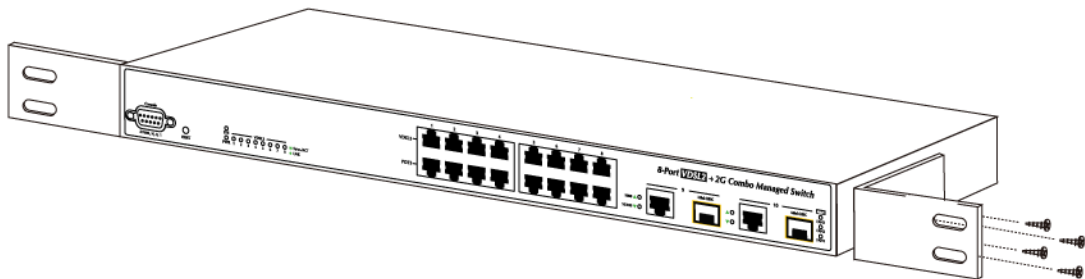


Figure 2-2-3: Attach brackets to VCO-8



You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-2-4 and Figure 2-2-5.

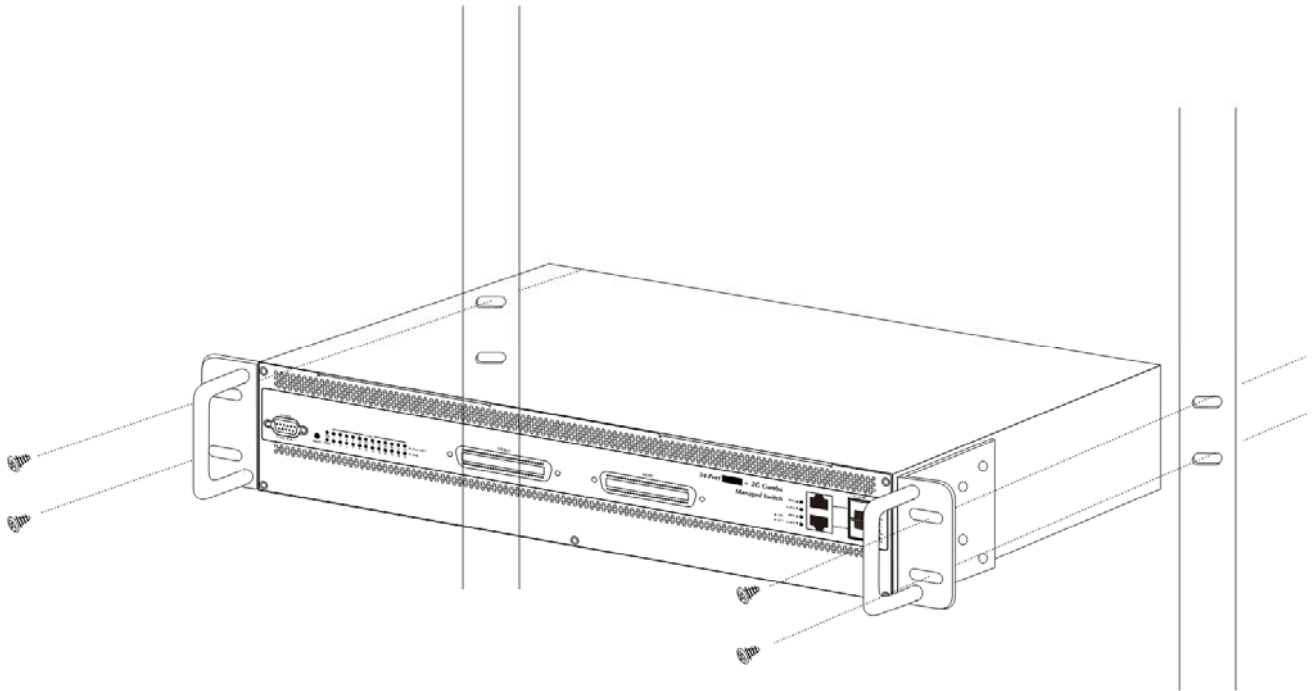


Figure 2-2-4: Mounting the VCO-24 series in a Rack

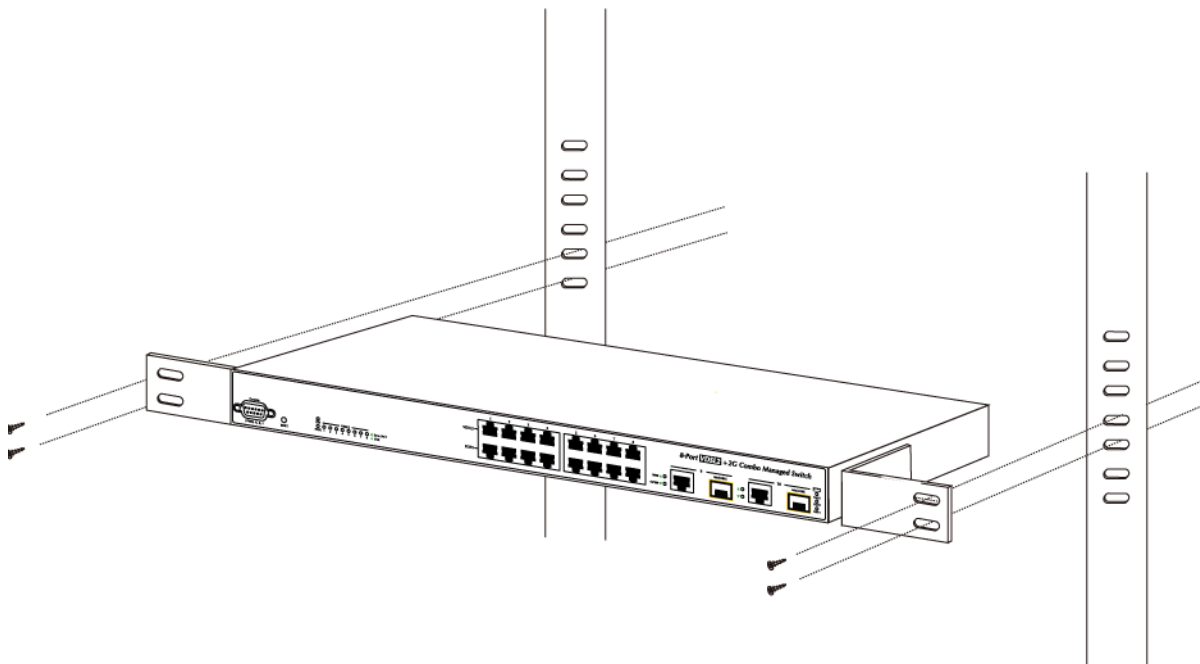


Figure 2-2-5: Mounting the VCO-8 in a Rack

Step6: Proceeds with the steps 4 and steps 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed Switch.

2.2.3 Installing the SFP transceiver

The sections describe how to insert an SFP transceiver into an SFP slot.

The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Managed Switch. As the [Figure 2-2-6](#) appears.

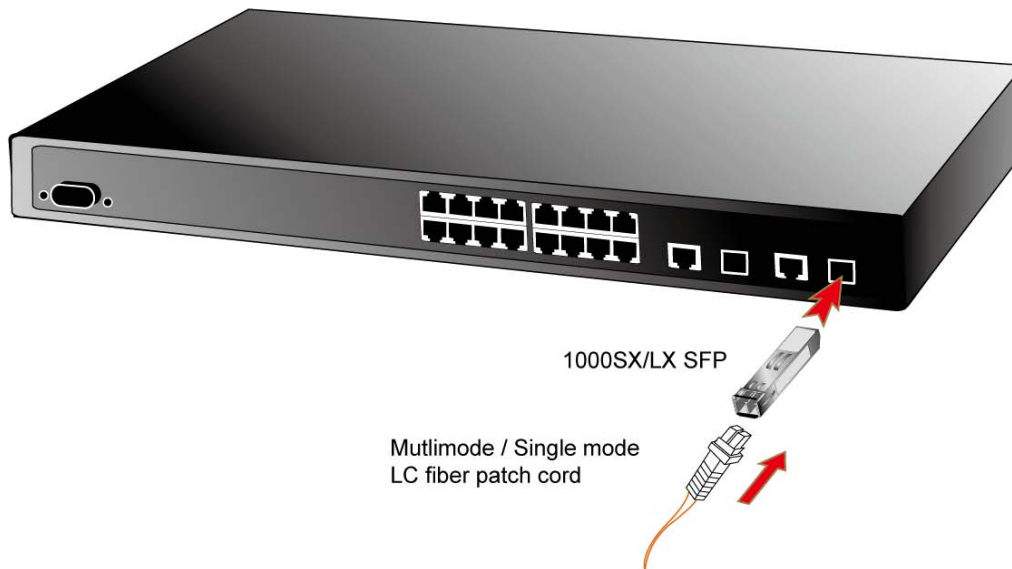


Figure 2-2-6: Plug-in the SFP transceiver

Approved SFP Transceivers

The Managed switches support both single mode and multi mode SFP transceivers. The following list of approved SFP transceivers is correct at the time of publication:

1000Base-SX/LX SFP transceiver:

- 1000BASE-SX SFP transceiver – Multi mode / 220m)
- 1000BASE-LX SFP transceiver - Single Mode / 10km)



It recommends using SFPs on the Switch. If you insert a SFP transceiver that is not supported, the Managed Switch will not recognize it.

Before connect to the other switches, workstation or Media Converter.

1. Make sure both side of the SFP transceiver are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.

2. Check the fiber-optic cable type match the SFP transceiver model.
 - To connect to **1000Base-SX** SFP transceiver, use the **multi-mode** fiber cable- with one side must be male duplex LC connector type.
 - To connect to **1000Base-LX** SFP transceiver, use the **single-mode** fiber cable-with one side must be male duplex LC connector type.

Connect the fiber cable

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a Media Converter.
3. Check the LNK/ACT LED of the SFP slot on the front of the Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link failed. Co works with some fiber-NICs or Media Converters, set the Link mode to “1000 Force” is needed.

Remove the transceiver module

1. Make sure there is no network activity by consult or check with the network administrator. Or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.
3. Turn the handle of the SFP transceiver to horizontal.
4. Pull out the module gently through the handle.

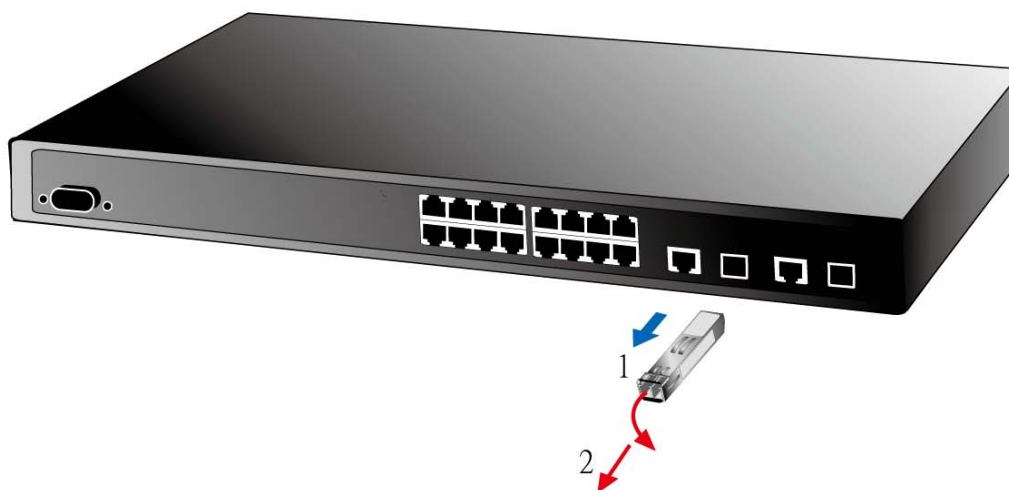


Figure 2-2-7: Pull out the SFP transceiver



Note

Never pull out the module without pull the handle or the push bolts on the module. Direct pull out the module with violent could damage the module and SFP module slot of the Managed Switch.

2.3 Wiring for VDSL2 Ports

The VDSL2 port of VCO-24 series uses one RJ-21 (Telco 50) connector to connect to a patch panel then link up to 24 VDSL CPEs and the VDSL2 port of VCO-8 uses eight RJ-11 connectors which can be just directly connected to the remote CPEs through structured or unstructured wiring, such as existing telephone lines. The link between the VDSL2 CO Switch port and each CPE can reach speeds of up to 100/100 Mbps under 1000 feet (300 meters) with profile 30a or 18/1 Mbps over distances of up to 5000 feet (1500 meters). You can hot swap the VDSL2 CPEs without powering down the Managed Switch or disrupting the other switch ports.

Each VCO-8 and VCO-24 VDSL2 Managed Switch series had built-in **Pain Old Telephone service (POTS)** splitter to transmit both VDSL2 traffic and telephone services, such as voice or Fax, through same phone wire. The splitter routes VDSL2 data (high-frequency) and voice (low-frequency) traffic from the telephone line and **Private Branch eXchange (PBX)** switch or **Public Switched Telephone Network (PSTN)**.

The connection diagrams are as the following.

■ VCO-24 VDSL2 and POTS connection

For the 24-Port VDSL or 24-PORT POTS, there are 24 pairs are used for tip and ring. The top row of the RJ-21(Telco-50) connector is tip and the bottom row is ring. [Figure 2-3-1](#) shows the pin-out convention for the RJ-21 connector.

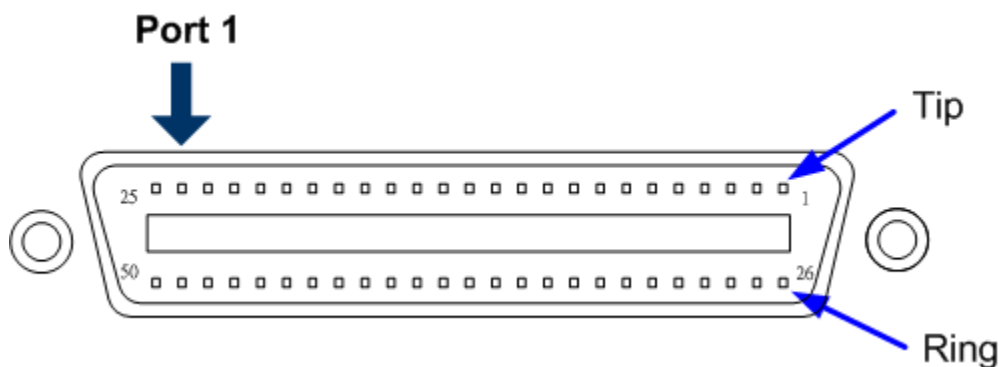


Figure 2-3-1: Pin-out convention for the RJ-21 connector of VCO-24



To get the pin assignment of the VDSL/POTS port numbers to the pin numbers on the RJ-21 of the VCO-24, please refer to [APPENDIX A.3](#) for more detail.

The VDSL port and POTS port of VCO-24 series always connects to a patch panel. The connection between the VCO-24 series and the patch panel is made by an RJ-21 Category 5 Telco interface connector and cable, as shown in [Figure 2-3-2](#) and [Figure 2-3-3](#).

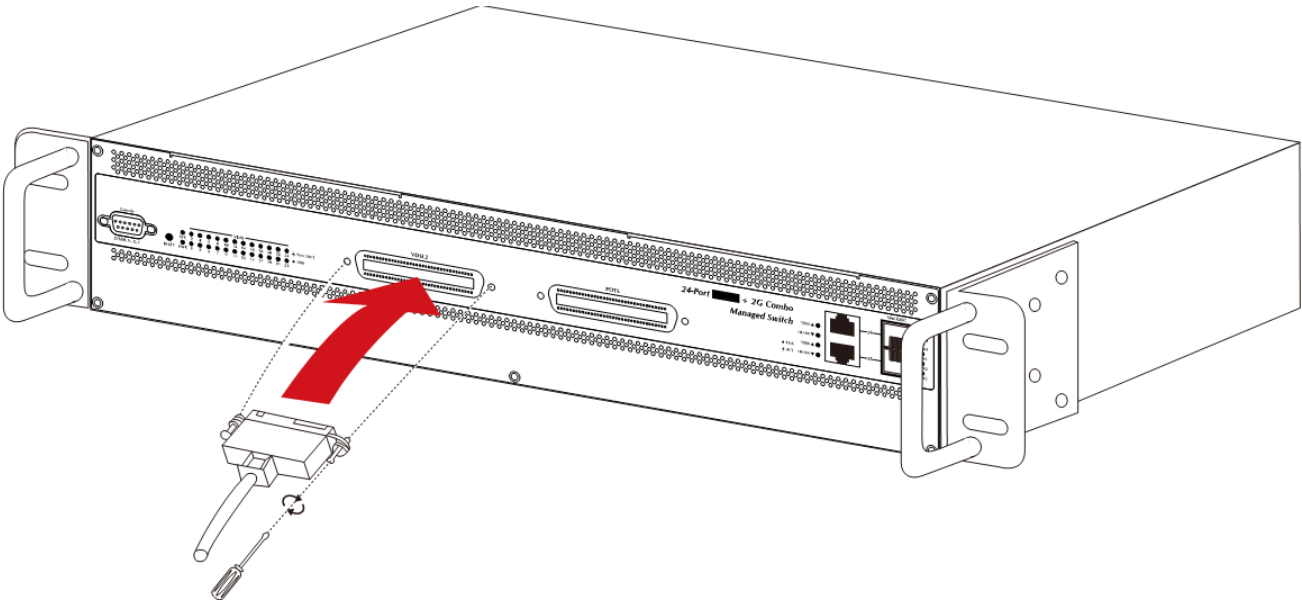


Figure 2-3-2: RJ-21 connect to VCO-24 series

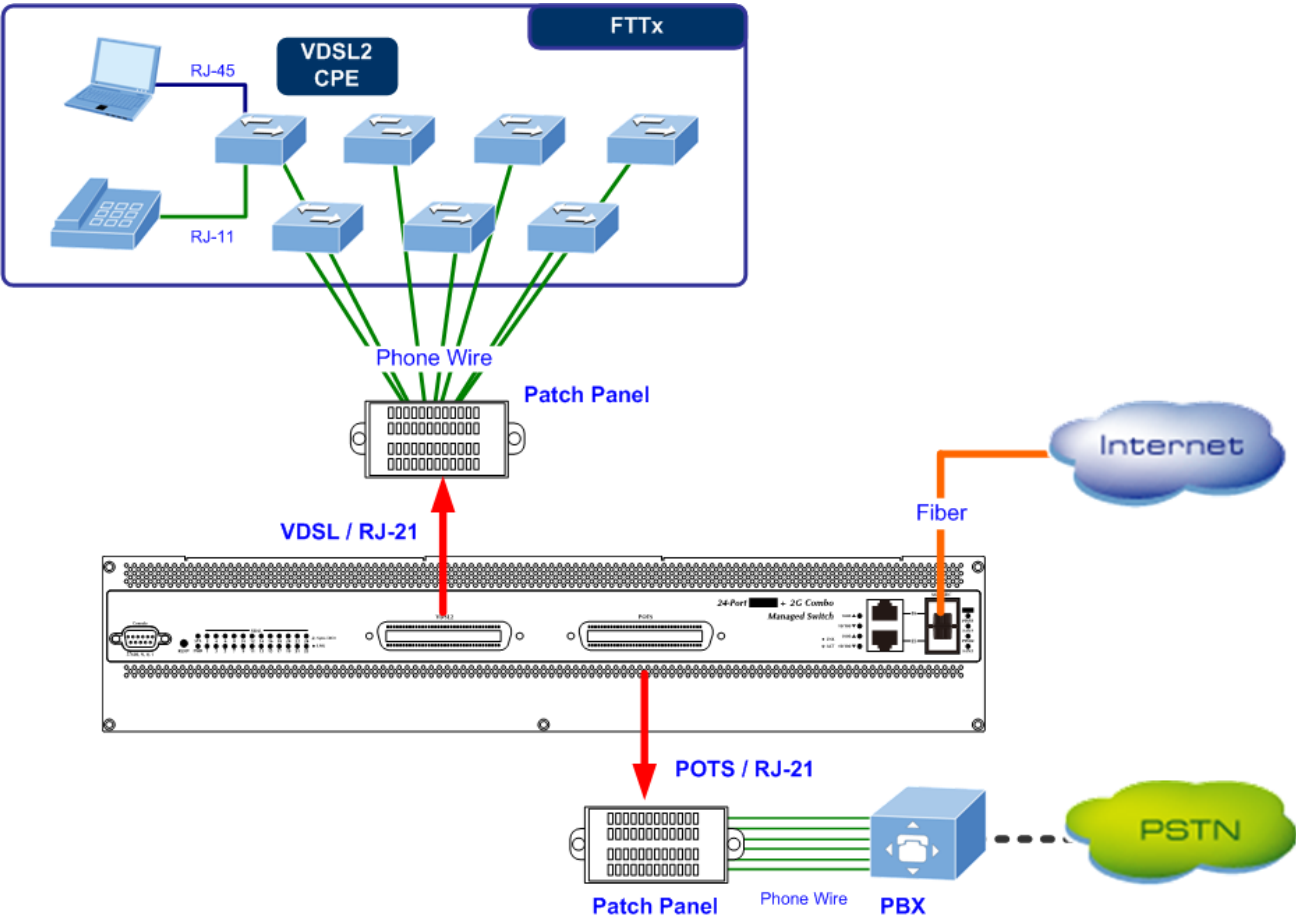


Figure 2-3-3: VCO-24 VDSL2 connection

■ VCO-8 VDSL2 connection

The VDSL2 port of VCO-8 uses eight RJ-11 connectors which can be just directly connected to the remote CPEs through existing telephone lines.

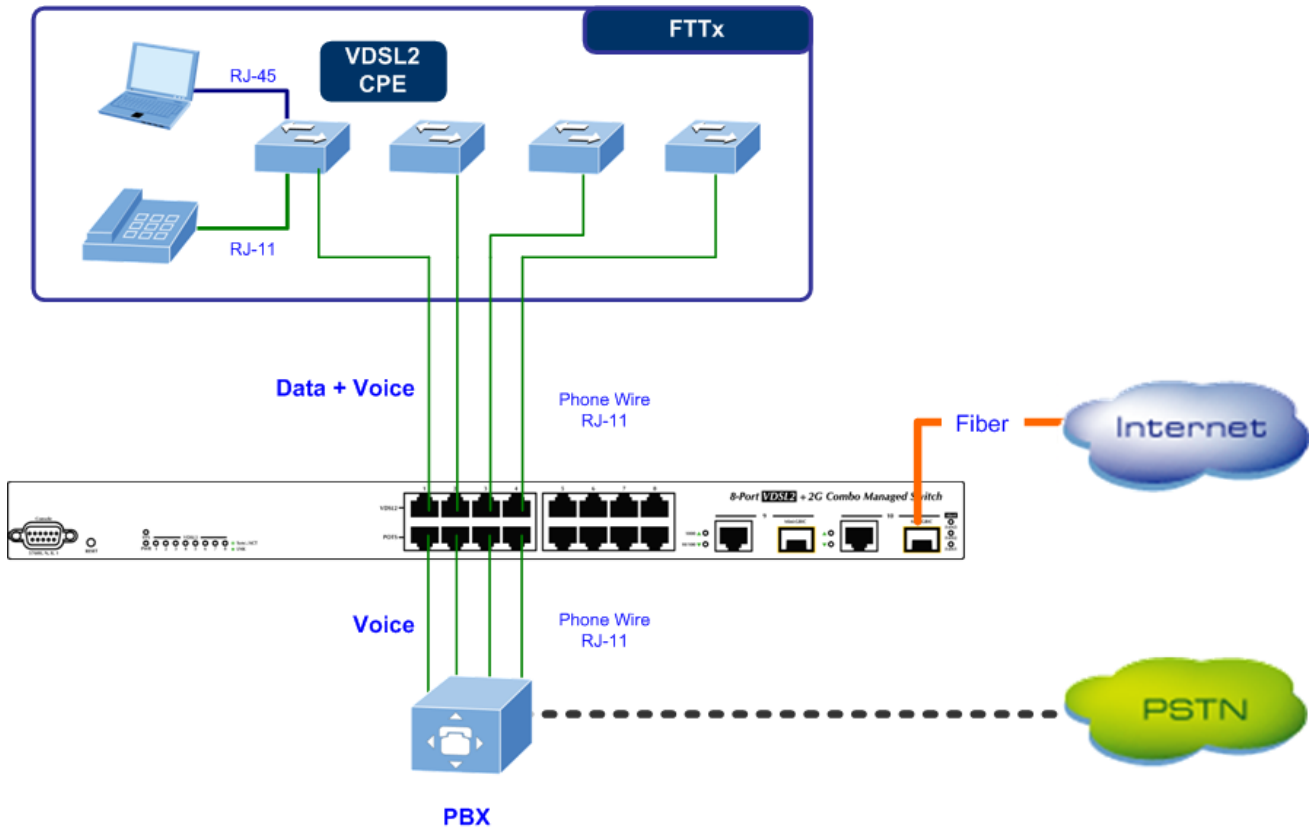


Figure 2-3-4: VCO-8 VDSL2 connection

If the port is connected but the relevant LED is dark, check the following items:

1. The VDSL2 Switch and the connected device's power are on or not.
2. The connecting cable is good and with correct type.
3. The cable is firmly seated in its connectors in the Managed Switch and in the associated device.
4. The connecting device, including any network adapter is well installed and functioning.
5. Confirm the VDSL2 CPE device is implemented within the scope of operative without interference.
6. Check the CPE's external splitter is installed well or not if CPE does not support internal splitter

3. SWITCH MANAGEMENT

This chapter explains the methods that you can use to configure management access to the Managed Switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (work-station or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Administration Console Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- **Workstations** of subscribers running Windows 98/ME, NT4.0, 2000/XP, MAC OS9 or later, Linux, UNIX or other platform compatible with **TCP/IP** protocols.
- **Workstation** installed with **Ethernet NIC** (Network Interface Card)
- Ethernet Port connect
 - Network cables - Use standard network (UTP) cables with RJ45 connectors.
- Above Workstation installed with **WEB Browser** and **JAVA Runtime Environment** Plug-in
- **Serial Port** connect
 - Above PC with COM Port (DB-9 / RS-232) or USB-to-RS-232 converter



It is recommended to use Internet Explore 6.0 or above to access Managed Switch.

3.2 Management Access Overview

The Managed Switch gives you the flexibility to access and manage it using any or all of the following methods:

- **Web browser** interface
- **An external SNMP-based network management application**
- **An administration console**

The administration console and Web browser interface support are embedded in the Managed Switch software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)
Console	• No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems • Secure	• Must be near switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow

Table 3-1: Management Methods Comparison

3.3 Web Management

The Managed Switch offers management features that allow users to manage the Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After you set up your IP address for the switch, you can access the Managed Switch's Web interface applications directly in your Web browser by entering the IP address of the Managed Switch.

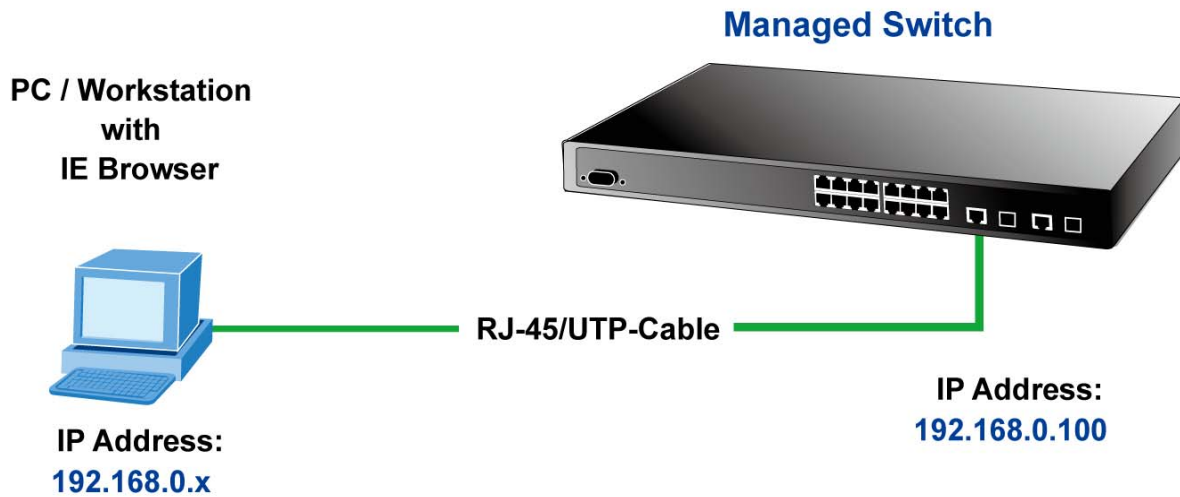


Figure 3-3-1: Web management

You can then use your Web browser to list and manage the Managed Switch configuration parameters from one central location, just as if you were directly connected to the Managed Switch's console port. Web Management requires either **Microsoft Internet Explorer 6.0** or later, **Safari** or **Mozilla Firefox 2.0** or later.



Figure 3-3-2: Web main screen of Managed Switch

3.4 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the Managed Switch, such as SNMPc Network Manager, HP Openview Network Node Management (NNM) or What'sup Gold. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP Network Management Station only knows the set community string, it can read and write to the MIBs. However, if it only configures the get community string, it can only read MIBs. The default get and set community strings for the Managed Switch are not configured.

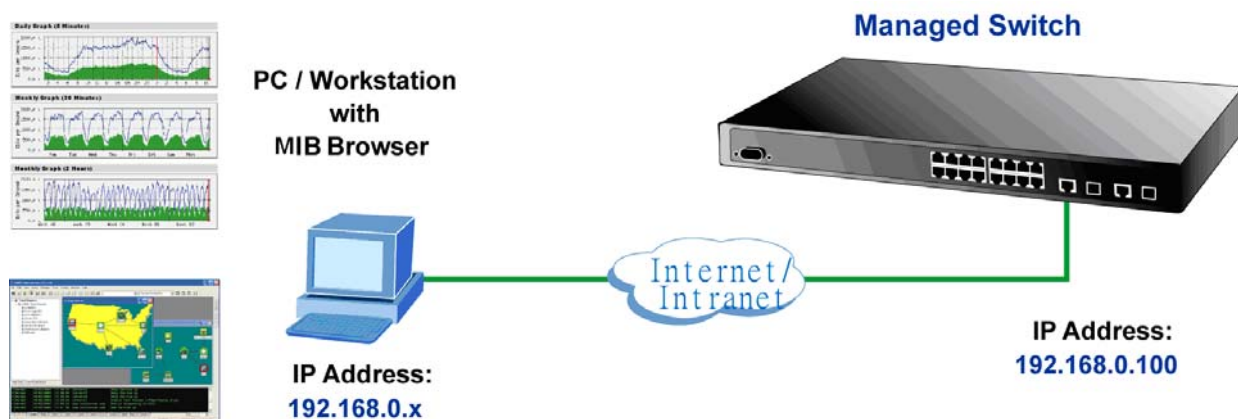


Figure 3-4-1 SNMP management

3.5 Administration Console

The administration console is an internal, text-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the switch's console (serial) port. There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to **Chapter 5 Console Management**.



Figure 3-5-1 Console management

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as **HyperTerminal**) to the Managed Switch console (serial) port.

When using this management method, a **straight DB9 RS-232 cable** is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

- **57600 bps**
- **8 data bits**
- **No parity**
- **1 stop bit**



Figure 3-5-2 Terminal parameter settings

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

3.6 Protocols

The Managed Switch supports the following protocols:

- Virtual terminal protocols, such as Telnet
- Simple Network Management Protocol (SNMP)

3.6.1 Virtual Terminal Protocols

A virtual terminal protocol is a software program, such as **Telnet**, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the Managed Switch before you can establish access to it with a virtual terminal protocol.



Terminal emulation differs from a virtual terminal protocol in that you must connect a terminal directly to the console (serial) port.

To access the Managed Switch through a Telnet session:

1. Be Sure of the Managed Switch is configured with an IP address and the Managed Switch is reachable from a PC.
2. Start the Telnet program on a PC and connect to the Managed Switch.

The management interface is exactly the same with RS-232 console management.

3.6.2 SNMP Protocol

Simple Network Management Protocol (SNMP) is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

3.6.3 Management Architecture

All of the management application modules use the same Messaging Application Programming Interface (MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (console port, for example) are immediately displayable by the other management methods (for example, SNMP agent of Web browser). The management architecture of the switch adheres to the IEEE open standard. This compliance assures customers that the Managed Switch is compatible with, and will interoperate with other solutions that adhere to the same open standard.

4. WEB-BASED MANAGEMENT

This section introduces the configuration and functions of the Web-based management.

4.1 About Web-based Management

The Managed Switch offers management features that allow users to manage the Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-based Management supports Internet Explorer 6.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

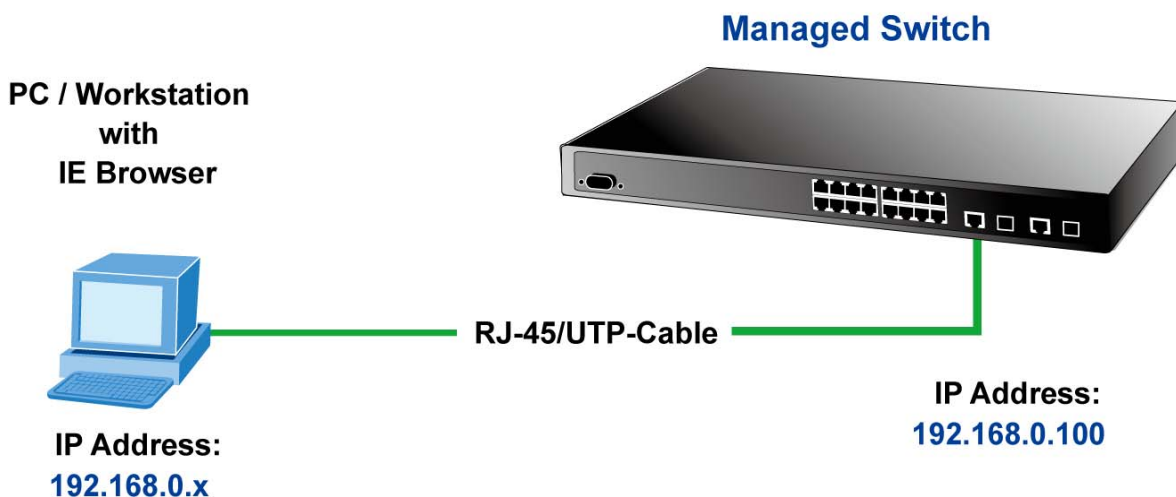


By default, IE 6.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The Managed Switch can be configured through an Ethernet connection, make sure the manager PC must be set on same the IP subnet address with the Managed Switch.

For example, the default IP address of the Managed Switch is **192.168.0.100**, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the Managed Switch to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.



4.1.1 Requirements

- Workstations of subscribers running Windows 98/ME, NT4.0, 2000/2003/XP, MAC OS9 or later, Linux, UNIX or other platform compatible with TCP/IP protocols.
- Workstation installed with Ethernet NIC (Network Card).
- **Ethernet Port connect**
 - Network cables - Use standard network (UTP) cables with RJ45 connectors.
 - Above PC installed with WEB Browser and JAVA Runtime Environment Plug-in.



It is recommended to use Internet Explorer 6.0 or above to access VCO-8 /VCO-24 series Managed Switch.

4.1.2 Logging on the switch

1. Use Internet Explorer 6.0 or above Web browser. Enter the factory-default IP address to access the Web interface.
The factory-default IP Address as following:

http://192.168.0.100

2. When the following login screen appears, please enter the default username "**admin**" with password "**admin**" (or the username/password you have changed via console) to login the main screen of Managed Switch. The login screen in [Figure 4-1-1](#) appears.



Figure 4-1-1: Login screen

Default username: **admin**

Default password: **admin**

1. After entering the username and password, the main screen appears as [Figure 4-1-2](#).



Figure 4-1-2: Web main page

2. The Switch Menu on the left of the Web page let you access all the commands and statistics the Switch provides.

Now, you can use the Web management interface to continue the switch management or manage the Managed Switch by Web interface. The Switch Menu on the left of the web page let you access all the commands and statistics the Managed Switch provides.



1. It is recommended to use Internet Explore 6.0 or above to access Managed Switch.
2. The changed IP address take effect immediately after click on the **Apply** button, you need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.
4. The WEB configuration and CLI command of VCO-8 are the same with VCO-24 except Power/Fan module detection feature, so the VCO-8 will be the example to describe how to configure switch and is also applicable to VCO-24 Managed Switch.

4.1.3 Main WEB PAGE

The Managed Switch provides a Web-based browser interface for configuring and managing it. This interface allows you to access the Managed Switch using the Web browser of your choice. This chapter describes how to use the Managed Switch's Web browser interface to configure and manage it.

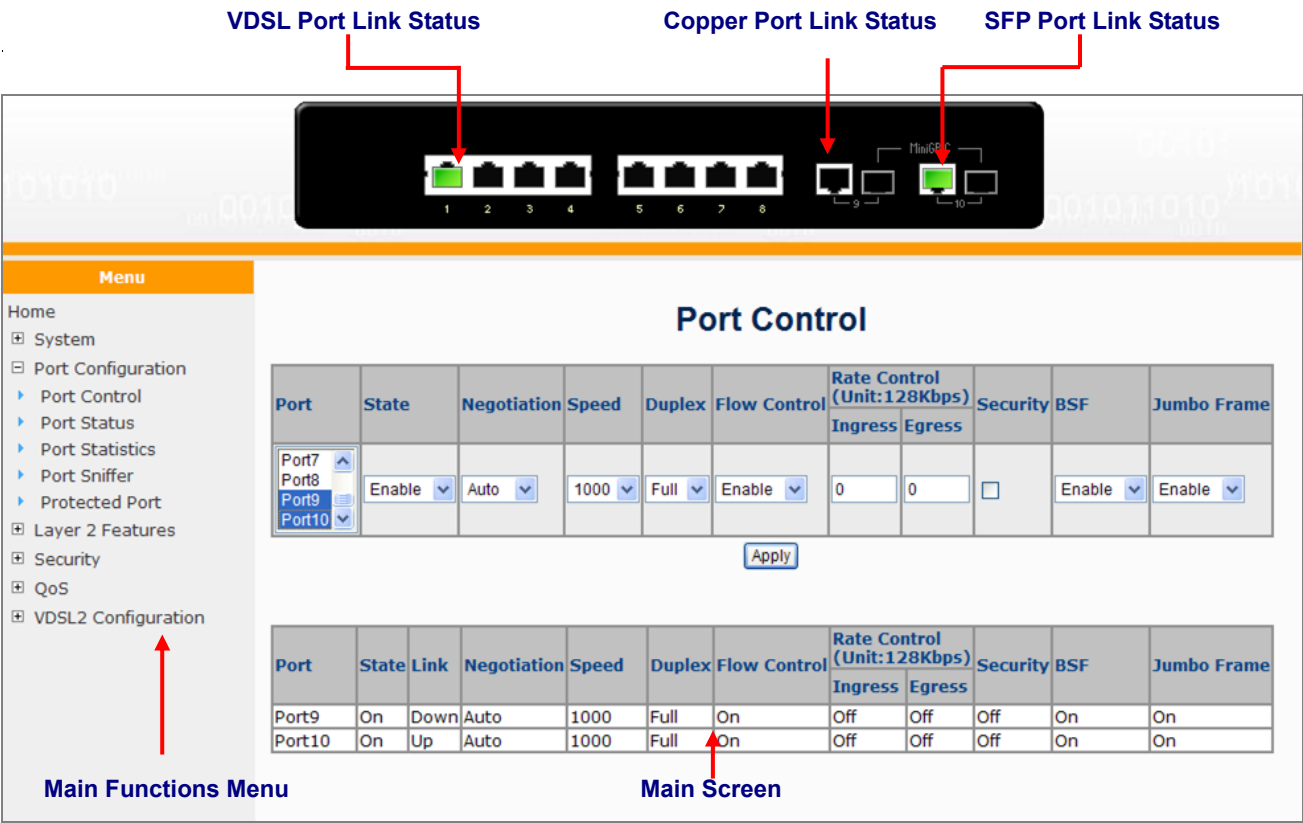


Figure 4-1-3: Main Page

Panel Display

The web agent displays an image of the Managed Switch's ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the **Port Statistics** page.

The port states are illustrated as follows:

State	Disabled	Down	Link
RJ-45 Ports			
SFP Ports			

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the Managed Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can setup the Managed Switch by select the functions those listed in the Main Function. The screen in [Figure 4-1-4](#) appears.

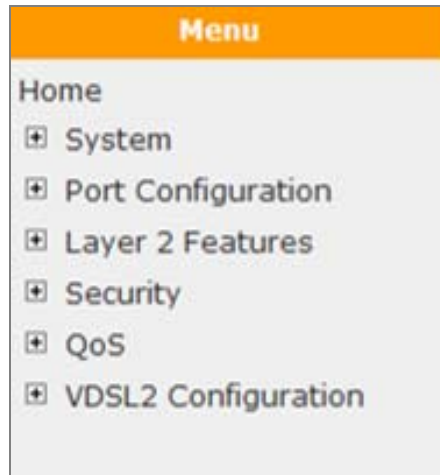


Figure 4-1-4: VCO-8 / VCO-24 Managed Switch Main Functions Menu

4.2 System

Use the System menu items to display and configure basic administrative details of the Managed Switch. Under System the following topics are provided to configure and view the system information: This section has the following items:

- | | |
|-------------------------------|---|
| ■ System Information | Provides basic system description, including contact information. |
| ■ IP Configuration | Set the IP address for management access. |
| ■ Console Port Info | Display the required console settings on the Managed Switch. |
| ■ SNMP Configuration | Configure SNMP agent and SNMP Trap. |
| ■ Syslog Setting | Configure logging of messages and assign IP address of remote Syslog servers. |
| ■ Firmware Upgrade | Upgrade the firmware via TFTP server or Web Brower file transfer. |
| ■ Configuration Backup | Save/view the Managed Switch configuration to remote host.
Upload the switch configuration from remote host. |
| ■ Factory Default | Reset the configuration of the Managed Switch. |
| ■ System Reboot | Restart the Managed Switch. |

4.2.1 System Information

In System information, it has two parts of setting – **Basic** and **Misc Config**. We will describe the configure detail in following.

4.2.1.1 Basic

The Basic System Info page provides information for the current device information. Basic System Info page helps a switch administrator to identify the model name, firmware / hardware version and MAC address. The screen in [Figure 4-2-1](#) appears.

System Information	
Basic	Misc Config
Model Name	8+2G
Description	8-Port VDSL2 + 2G TP/SFP Combo Managed Switch
MAC Address	00:nn:nn:00:00:06
Firmware Version	1.08
Hardware Version	1.0
Build Firmware Date	100107_1946

Figure 4-2-1: Basic System Information screenshot

The page includes the following fields:

Object	Description
Model Name:	Display the system name of the Managed Switch.
Description:	Describe the Managed Switch.
MAC Address:	Display the unique hardware address assigned by supplier.
Firmware Version:	Display the Managed Switch's firmware version.
Hardware Version:	Display the Managed Switch's hardware version.
Build Firmware Date:	Display the date information of the firmware.

4.2.1.2 Misc Config

Choose **Misc Config** from System Information of Managed Switch, the screen in [Figure 4-2-2](#) appears.

System Information

Basic

Misc Config

☐ MAC Table Address Entry

Age-Out Time: seconds (6~1572858,must multiple of 6,default is 300s)

Turn On Port Interval: seconds (0~3600 seconds, interval time between turning off and turning on port for flooding CPU port, 0:disable)

Broadcast Storm Filter Mode:

OFF

Broadcast Storm Filter Packet select

☐ Broadcast Packets

☐ IP Multicast

☐ Control Packets

☐ Flooded Unicast/Multicast Packets

Collisions Retry Forever :

Disable

Hash Algorithm :

CRC-Hash

IP/MAC Binding :

Disable

802.1x Protocol :

Disable

Apply

Default

Help

Figure 4-2-2: Switch Misc Config screenshot

The page includes the following fields:

Object	Description
MAC Address Age-out Time	Type the number of seconds that an inactive MAC address remains in the switch's address table. The value is a multiple of 6. Default is 300 seconds.
Broadcast Storm Filter	To configure broadcast storm control, enable it and set the upper threshold for

Mode	individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold values are 1/2, 1/4, 1/8, 1/16 and OFF. Default is "OFF".
Broadcast Storm Filter Packets Select	To select broadcast storm Filter Packets type. If no packets type by selected, mean can not filter any packets .The Broadcast Storm Filter Mode will show OFF. The selectable items as below: • Broadcast Packets • IP Multicast • Control Packets • Flooded Unicast / Multicast Packets
Collision Retry Forever	Provide Collision Retry Forever function: "Disable" or 16, 32, 48 collision numbers on Managed Switch. If this function is disabled, when a packet meet a collision, the Managed Switch will retry 6 times before discard the packets. Otherwise, the Managed Switch will retry until the packet is successfully sent. Default value is 16.
Hash Algorithm	Provide MAC address table Hashing setting on Managed Switch; available options are CRC-Hash and DirectMap. Default mode is CRC-Hash.
IP/MAC Binding	Enable / Disable IP MAC Binding function.
802.1X Protocol	Enable / Disable 802.1X protocol.
Apply button	Press the button to complete the configuration.

4.2.1.3 Module Info

This section provides current status of power supply unit from VCO-24, the screen in [Figure 4-2-3](#) appears and [table 4-2-1](#) describes the power and fan module Status object of VCO-24.

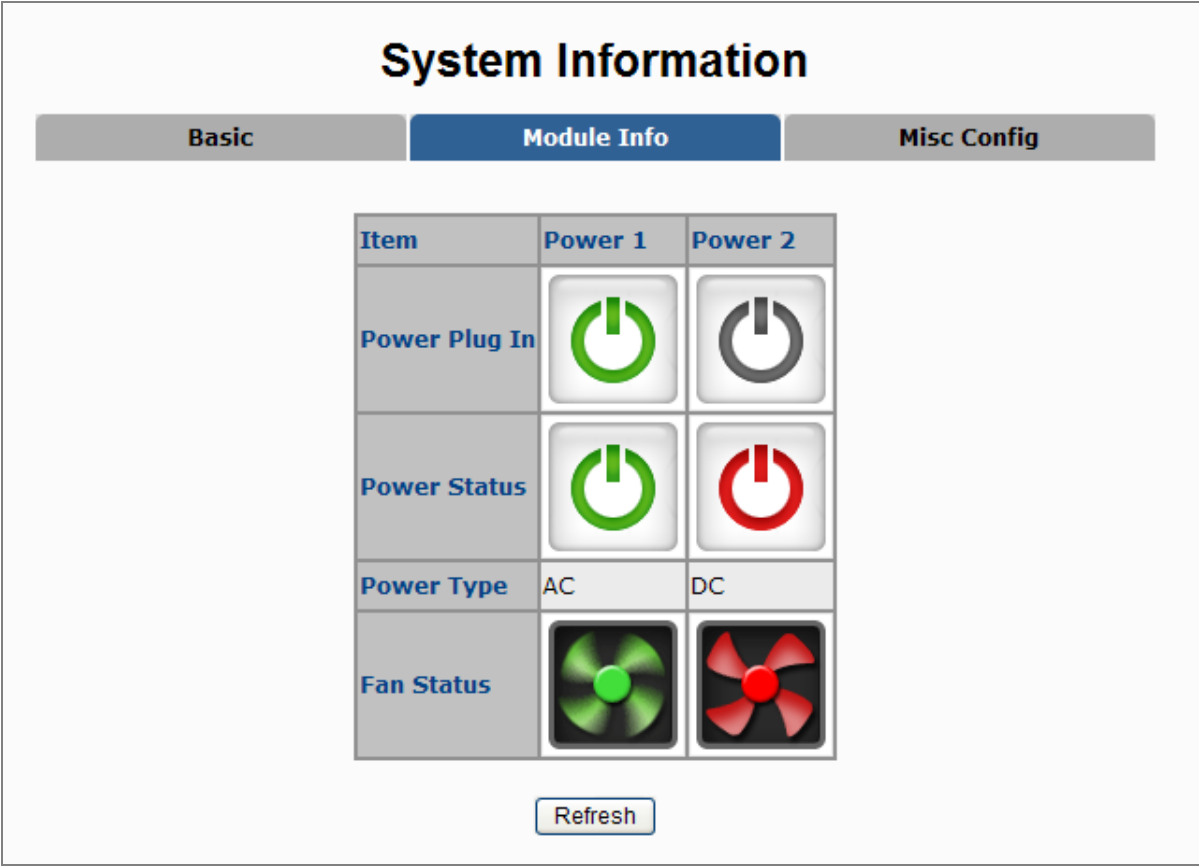


Figure 4-2-3 Chassis Status Web Page Screen

Item	Power 1	Power 2
Power Plug In	Gray: indicate the power supply unit not install into the VCO-24. Green: indicate the power supply unit install into the VCO-24.	
Power Status	Gray: indicate the power supply unit not install into the VCO-24. Green: indicate the power supply unit has power. Red: indicate the power supply unit has no power or failure.	
Power Type	AC: indicate the AC power supply unit installed into the VCO-24. DC: indicate the DC power supply unit installed into the VCO-24.	
Fan Status	Gray: indicate the fan unit not install into the VCO-24. Green: indicate the fan is operation normally. Red: indicate the fan is failure.	

Table 4-2-1 Descriptions of the Chassis Status Web Page Screen Objects



Once, installed the AC or DC power supply unit into VCO-24, the fan will start to working. Even, the AC or DC power supply unit has no power.

4.2.2 IP Configuration

The Managed Switch is a network device which needs to be assigned an IP address for being identified on the network. Users have to decide a means of assigning IP address to the Managed Switch.

IP address overview

What is an IP address?

Each device (such as a computer) which participates in an IP network needs a unique "address" on the network. It's similar to having a US mail address so other people have a know way to send you messages. An IP address is a four byte number, which is usually written in "dot notation" - each of the bytes' decimal value is written as a number, and the numbers are separated by "dots" (aka periods). An example: 199.25.123.1

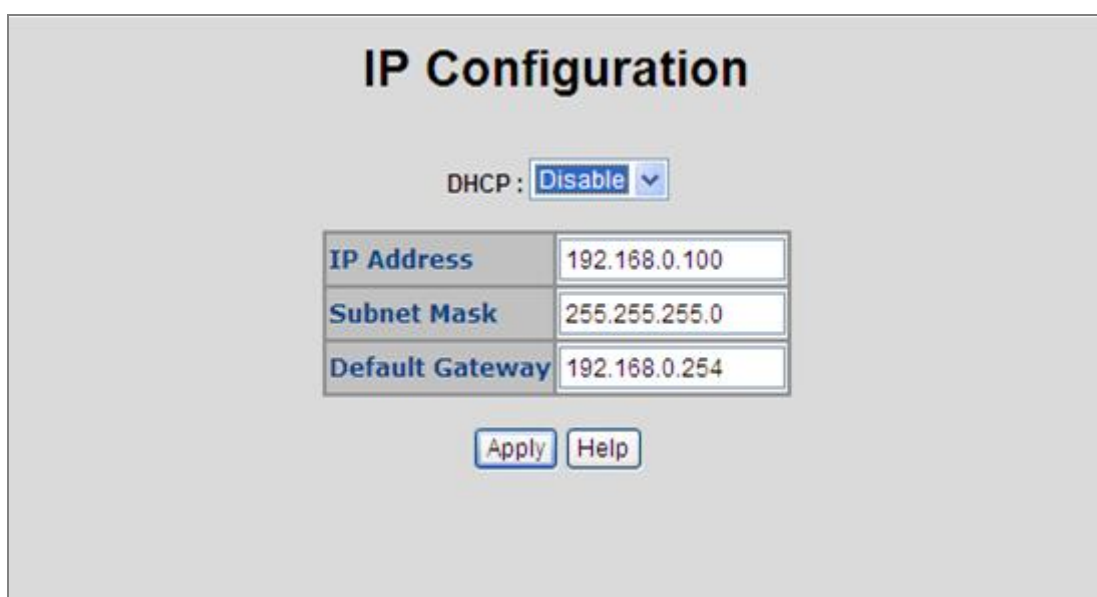
How do I get one for this box?

The IP addresses on most modern corporate nets are assigned by an employee called a "Network Administrator", or "Sys. Admin". This person assigns IP addresses and is responsible for making sure that IP addresses are not duplicated - If this happens one or both machines with a duplicate address will stop working.

Another possibility is getting your address assigned to you automatically over the net via DHCP protocol. Enable DHCP function, and reset the machine. If your network is set up for this service, you will get an IP address assigned over the network. If you don't get an address in about 30 seconds, you probably don't have DHCP server.

■ IP Configuration

The IP Configuration includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration. Fill up the IP Address, Subnet Mask and Gateway for the device. The screen in [Figure 4-2-4](#) appears.



The screenshot shows a web-based configuration interface titled "IP Configuration". At the top, there is a "DHCP:" label followed by a dropdown menu currently set to "Disable". Below this is a table with three rows for configuration:

IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.254

At the bottom of the interface are two buttons: "Apply" and "Help".

Figure 4-2-4: IP configuration interface

The page includes the following fields:

Object	Description
DHCP	Enable or disable the DHCP client function. When DHCP function is enabled, the Managed Switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks Apply, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabled, this switch is configured as a DHCP client. The network DHCP server will assign the IP address to the switch and display it in this column. The default IP is 192.168.0.100 or the user has to assign an IP address manually when DHCP Client is disabled.
Subnet Mask	Assign the subnet mask to the IP address. If DHCP client function is disabled, the user has to assign the subnet mask in this column field.
Gateway	Assign the network gateway for the switch. If DHCP client function is disabled, the user has to assign the gateway in this column field. The default gateway is 192.168.0.254.

4.2.3 Console Port Info

Console is a standard UART interface to communicate with Serial Port. You can use Windows HyperTerminal program to link the Managed Switch. The page displays the required console settings on the Managed Switch.

Console Information	
Baurate(bits/sec)	57600
Data Bits	8
Parity Check	none
Stop Bits	1
Flow Control	none

[Help](#)

Figure 4-2-5: Console Information interface

4.2.4 SNMP Configuration

4.2.4.1 SNMP Overview

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management Information Base (MIB) and network-management protocol:

- **Network management stations (NMSs)** : Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents** : Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)** : A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **network-management protocol** : A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get** -- Allows the NMS to retrieve an object instance from the agent.
- **Set** -- Allows the NMS to set values for object instances within an agent.
- **Trap** -- Used by the agent to asynchronously inform the NMS of some events. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

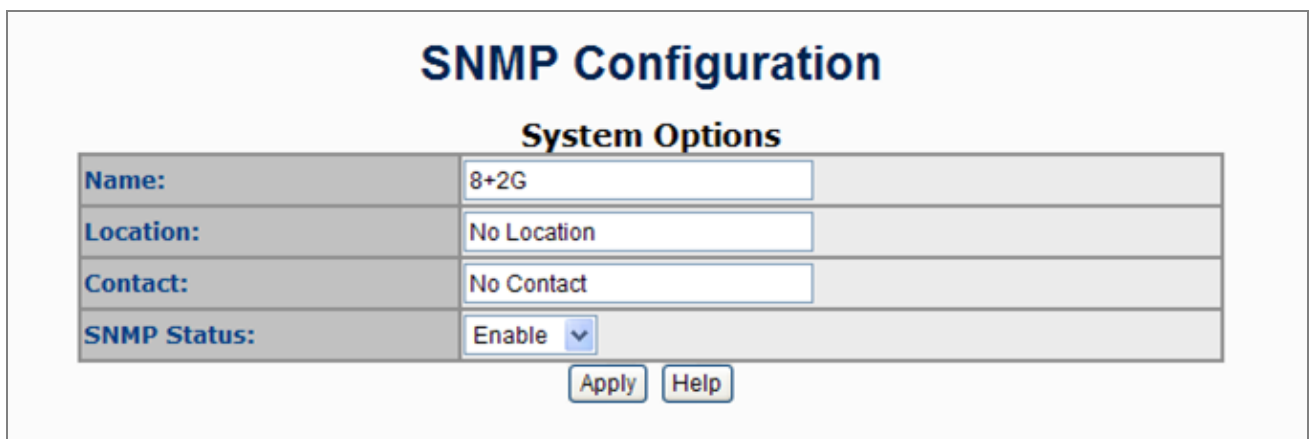
SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. The normal SNMP default communities are as below when configured:

- Write = **private**
- Read = **public**

4.2.4.2 System Options

Use this page to define management stations. You can also define a name, location, and contact person for the Managed Switch.



The image shows a web-based configuration interface titled "SNMP Configuration" with a sub-section "System Options". It contains four input fields: "Name:" with the value "8+2G", "Location:" with the value "No Location", "Contact:" with the value "No Contact", and "SNMP Status:" with a dropdown menu set to "Enable". Below the fields are two buttons: "Apply" and "Help".

Figure 4-2-6: SNMP configuration interface

The page includes the following fields:

Object	Description
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alphabetic character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Location	The physical location of this node (e.g., telephone closet, 3rd floor).
System Contact	The textual identification of the contact person for this managed node, together

	with information on how to contact this person.
SNMP Status	Indicates the SNMP mode operation. Possible modes are: - Enabled: Enable SNMP mode operation. - Disabled: Disable SNMP mode operation.

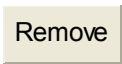
4.2.4.3 Community Strings

Community strings serve as passwords and can be entered as one of the following:



Figure 4-2-7: Community strings interface

The page includes the following fields:

Object	Description
Community Strings:	Here you can define the new community string set and remove the unwanted community string. - String: Fill the name string. - RO: Read only. Enables requests accompanied by this community string to display MIB-object information. - RW: Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
 button	Press the button to add the management SNMP community strings on the Managed Switch.
 button	Press the button to remove the management SNMP community strings that you defined before on the Managed Switch.

4.2.4.4 Trap Managers

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

Trap Managers

Current Managers:		New Manager:
192.168.0.52	<< Add << Remove	IP Address: Community:

Figure 4-2-8: Trap Managers interface

The page includes the following fields:

Object	Description
IP Address:	Enter the IP address of the trap manager.
Community:	Enter the community string for the trap station.

4.2.4.5 SNMPv3 Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.
The SNMPv3 Groups Configuration screen in [Figure 4-2-9](#) appears.

V3 Group

Current Strings:		SNMP Group
root_v1_root admin_v1_admin public_v1_public root_v2c_root admin_v2c_admin public_v2c_public	<< Add << Remove	Group Name: Input group-name V1 V2c USM: v1 Security Name: Input security-name

Figure 4-2-9: SNMPv3 Group configuration interface

The page includes the following fields:

Object	Description
Group Name:	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 15.
V1 V2c USM	Indicates the security model that this entry should belong to. Possible security models are: • v1: Reserved for SNMPv1. • v2c: Reserved for SNMPv2c. • usm: User-based Security Model (USM).
Security Name:	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 15.
Remove	Check to delete the entry. It will be deleted during the next save.

4.2.4.6 SNMPv3 View

Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Sub tree.

The SNMPv3 View Configuration screen in [Figure 4-2-10](#) appears.

V3 View

Current Strings:		SNMP View
<pre>all_included_1_80 mib2_included_1.3.6.1.2.1_fc system_included_1.3.6.1.2.1.1_fe</pre>	<< Add << Remove	View Name: Input view-name Included Excluded: included View Subtree(eg: 1.3.6.1.2.1) Input view-subtree View Mask(Hexadecimal Digits): Input view-mask

Figure 4-2-10: SNMPv3 View configuration interface

The page includes the following fields:

Object	Description
View Name:	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 15.
Included Excluded:	Indicates the view type that this entry should belong to. Possible view type are: • included: An optional flag to indicate that this view subtree should be included. • excluded: An optional flag to indicate that this view subtree should be excluded.
View Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*)
View Mask(Hexadecimal Digits):	View mask is defined in order to reduce the amount of configuration information required when fine-grained access control is required (e.g., access control at the object instance level)

4.2.4.7 SNMPv3 Access

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.

The SNMPv3 Access Configuration screen in [Figure 4-2-11](#) appears.

The figure shows a web-based configuration interface titled "V3 Access". It is divided into two main sections: "Current Strings" and "SNMP Access".

Current Strings: A list box containing the following strings:

- root_v1_noauth_all_all_all
- root_v2c_noauth_all_all_all
- admin_v1_noauth_all_none_all
- admin_v2c_noauth_all_none_all
- public_v1_noauth_system_none_system
- public_v2c_noauth_system_none_system

Below the list box are two buttons: "<< Add <<" and "Remove".

SNMP Access: A form with the following fields:

- Group Name: Input group-name
- V1|V2c|USM: v1 (dropdown menu)
- SNMP Access: noauth (dropdown menu)
- Read View: Input read-view
- Write View: Input write-view
- Notify View: Input notify-view

Figure 4-2-11: SNMPv3 Access configuration interface

The page includes the following fields:

Object	Description
Group Name:	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 15.
V1 V2c USM:	Indicates the security model that this entry should belong to. Possible security

	models are:
	• v1: Reserved for SNMPv1. • v2c: Reserved for SNMPv2c. • usm: User-based Security Model (USM)
	Indicates the security model that this entry should belong to. Possible security models are:
SNMP Access:	• noauth: None authentication and none privacy. • auth: Authentication and none privacy. • authpriv: Authentication and privacy.
Read View:	The name of the MIB views defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 16.
Write View:	The name of the MIB views defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 16.
Notify View:	Set up the notify view.
Remove	Check to delete the selected entry. It will be deleted during the next save.

4.2.4.8 SNMP V3 usm-user

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.

The SNMPv3 Users Configuration screen in [Figure 4-2-12](#) appears.

The screenshot shows the 'V3 usm-user' configuration window. It is divided into three main sections. On the left, under 'Current Strings:', there is a list box containing '(none)'. In the center, there are two buttons: '<< Add <<' and 'Remove'. On the right, under the heading 'SNMP usm-user', there are four configuration fields: 'SNMP User Name:' with a text input field containing 'Input user-name'; 'Auth Type:' with a dropdown menu set to 'none'; 'Auth Key(8~32):' with a text input field containing 'Input auth-key'; and 'Private Key(8~32):' with a text input field containing 'Input priv-key'.

Figure 4-2-12: SNMPv3 usm-user configuration interface

The page includes the following fields:

Object	Description
--------	-------------

SNMP User Name:	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 15.
Auth Type:	Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are: • none: None authentication protocol. • md5: An optional flag to indicate that this user using MD5 authentication protocol. The value of security level cannot be modified if entry is already existed. That means must first ensure that the value is set correctly.
Auth Key(8~32):	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32.
Private Key(8~32):	A string identifying the privacy pass phrase. The allowed string length is 8 to 32.
Remove	Check to delete the selected entry. It will be deleted during the next save.

4.2.5 Syslog Setting

The Syslog Setting page allows you to configure the logging of messages that are sent to remote syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.

Figure 4-2-13: Syslog Setting web interface

The page includes the following fields:

Object	Description
Syslog Server IP	IP address of syslog server.
Log level	• None: No send syslog message to syslog server, and Max Age parameters of the root bridge, regardless of how it is configured. • Major: only send major syslog to syslog server, e.g. link up/down, system warm/cold start • All: send all syslog messages to syslog server.

4.2.6 Firmware Upgrade

It provides the functions allowing the user to update the switch firmware via the **Trivial File Transfer Protocol (TFTP)** server. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

4.2.6.1 TFTP Firmware Upgrade

The **Firmware Upgrade** page provides the functions to allow a user to update the Managed Switch firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The screen in [Figure 4-2-14](#) appears.

Use this menu to download a file from specified TFTP server to the Managed Switch.

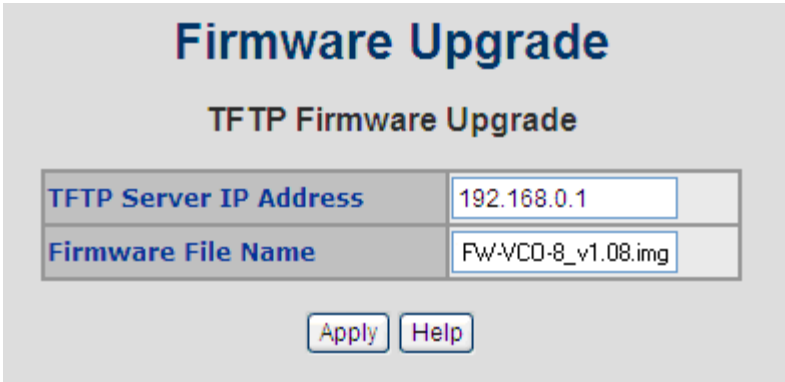


Figure 4-2-14: Firmware Upgrade interface

The page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in your TFTP server IP.
Firmware File Name:	Type in the name of the firmware image file to be updated.

4.2.6.2 HTTP Firmware Upgrade

The **HTTP Firmware Upgrade** page contains fields for downloading system image files from the Local File browser to the device. The Web Firmware Upgrade screen in [Figure 4-2-15](#) appears.



Figure 4-2-15: HTTP Firmware Upgrade interface

To open **Firmware Upgrade** screen perform the following:

1. Click System -> Web Firmware Upgrade.
2. The Firmware Upgrade screen is displayed as in [Figure 4-2-15](#).
3. Click the "Browse" button of the main page, the system would pop up the file selection menu to choose firmware.

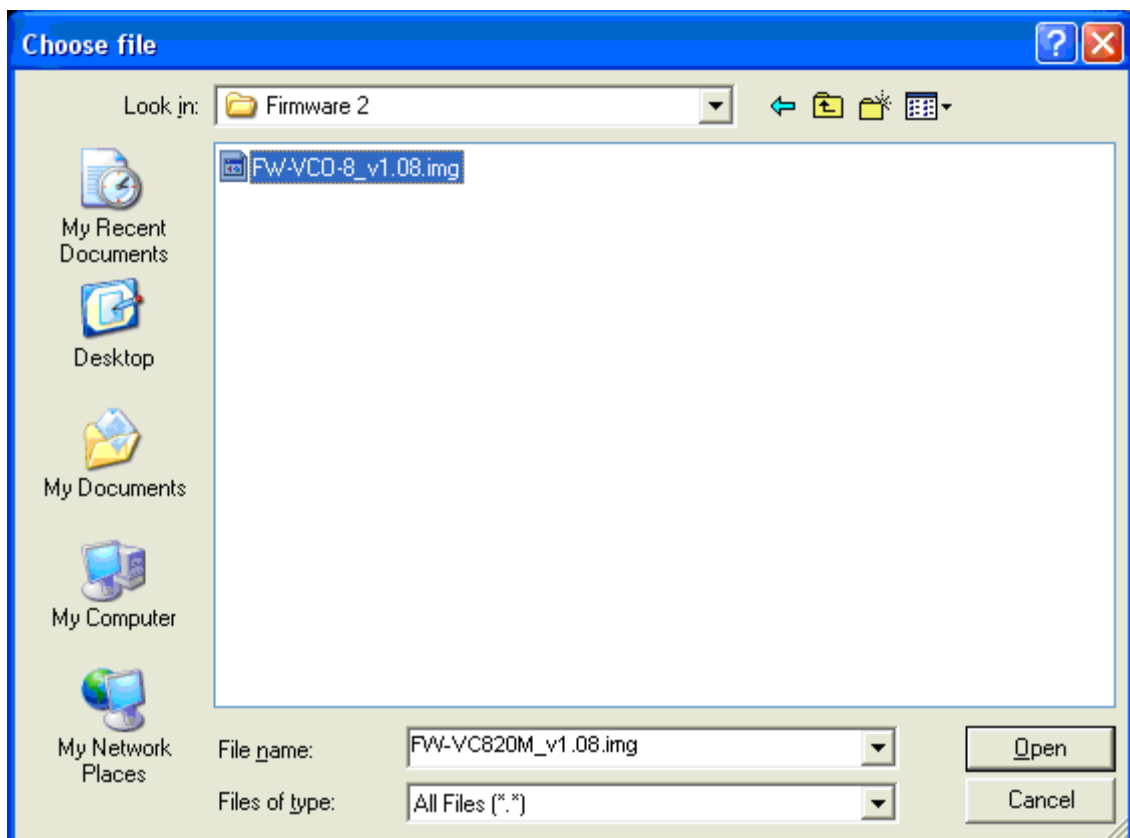


Figure 4-2-16: HTTP Firmware Upgrade selection window

4. Select on the firmware then click **“Submit”**, the Software Upload Progress would show the file upload status.



Firmware upgrade needs several minutes. Please wait a while, and then manually refresh the webpage.

4.2.7 Configuration Backup

4.2.7.1 TFTP Restore Configuration

You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first and the Managed Switch will get the configuration file and store to flash ROM.

Figure 4-2-17: TFTP Configuration Restore interface

The page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in the TFTP server IP.
Restore File Name:	Type in the correct file name for restoring.

4.2.7.2 HTTP Config File Restore

You can also restore the previous backup configuration from the current workstation utilize internet browser such as Microsoft Internet Explore or Mozilla Firefox, to recover the settings. Before doing that, you must locate the configuration file on the local management station first and the Managed Switch will get it back and store in flash ROM.

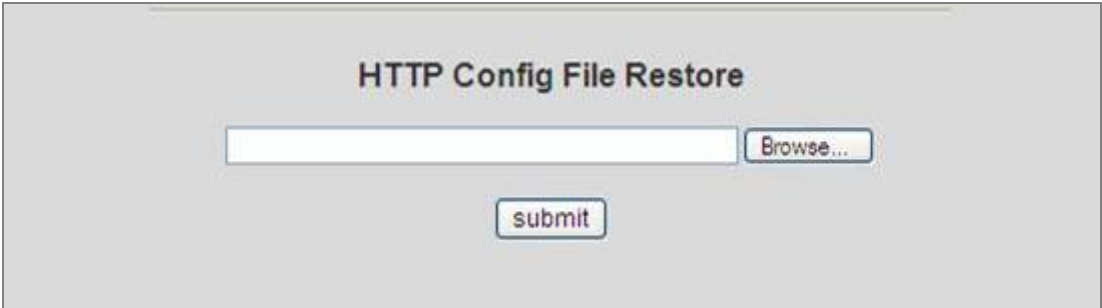


Figure 4-2-18: HTTP Configuration Restore interface

4.2.7.3 TFTP Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you to avoid wasting time on configuring the settings by backing up the configuration.

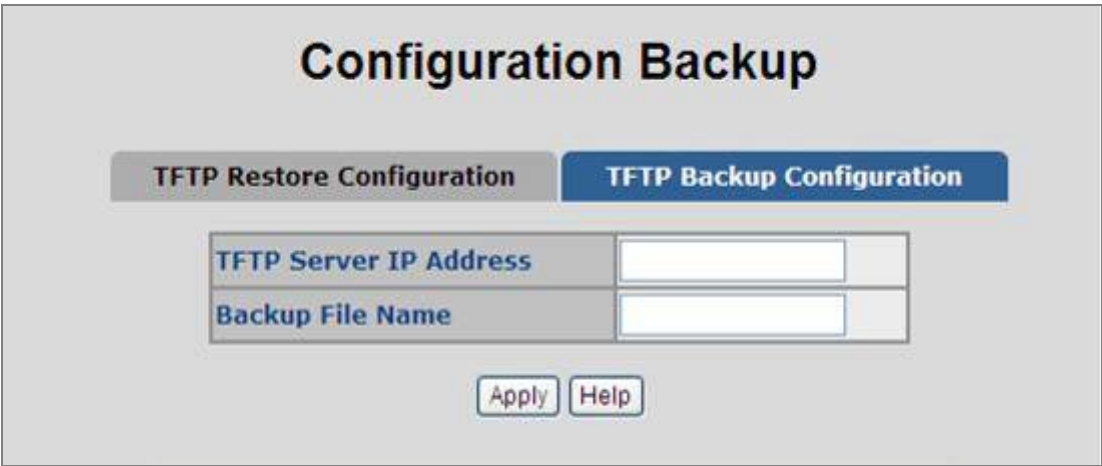


Figure 4-2-19: TFTP Configuration Backup interface

The page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in the TFTP server IP.
Backup File Name:	Type in the file name of configuration when backup on the TFTP server.

4.2.7.4 HTTP Config File Backup

This function allows backup the current configuration of the Managed Switch to the local management station. The screens in [Figure 4-2-20](#) and [Figure 4-2-21](#) appear.

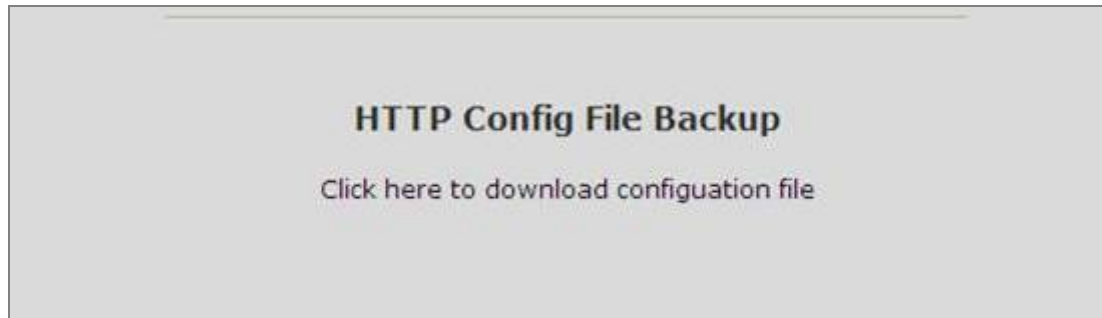


Figure 4-2-20: HTTP configuration file backup interface

Move the cursor to “[Click here to download configuration file](#)” and click. The backup configuration file will be packaged as a “config.tar” file as default.

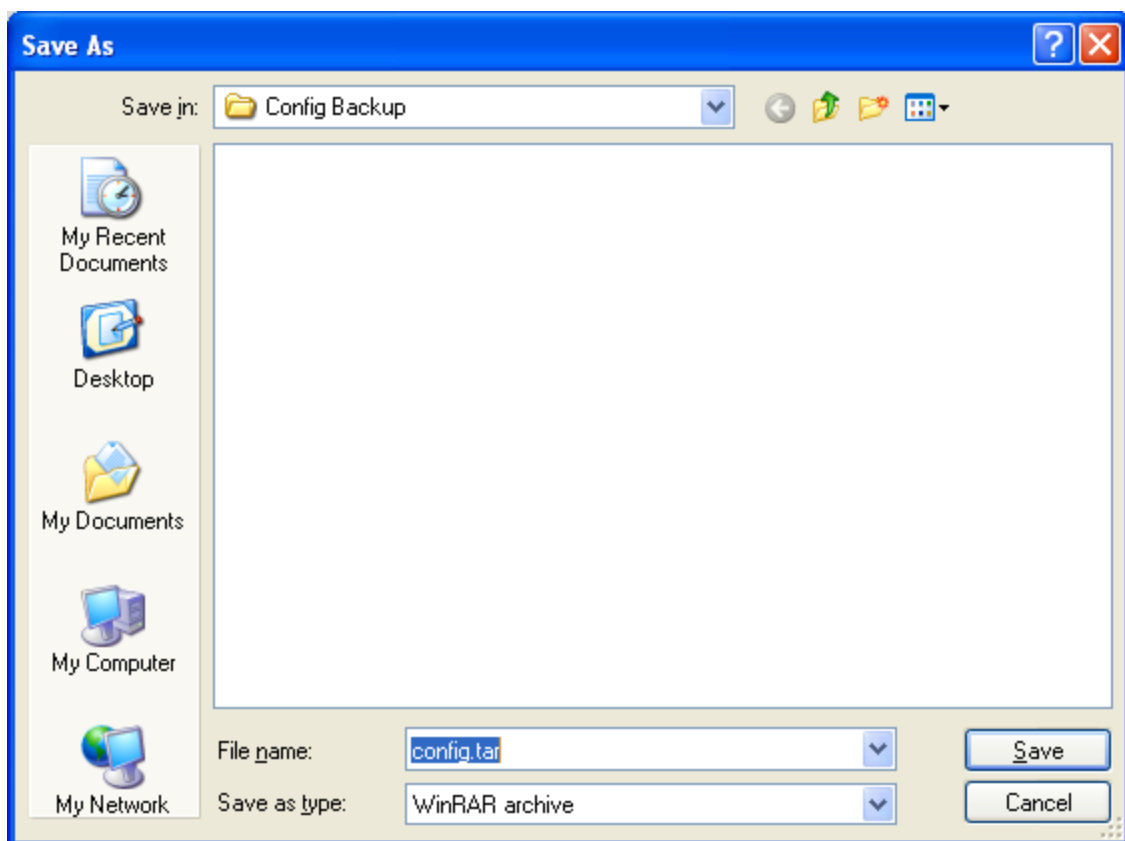


Figure 4-2-21: HTTP Configuration Backup window

4.2.8 Factory Default

Reset switch to default configuration. Click  to reset all configurations to the default value.

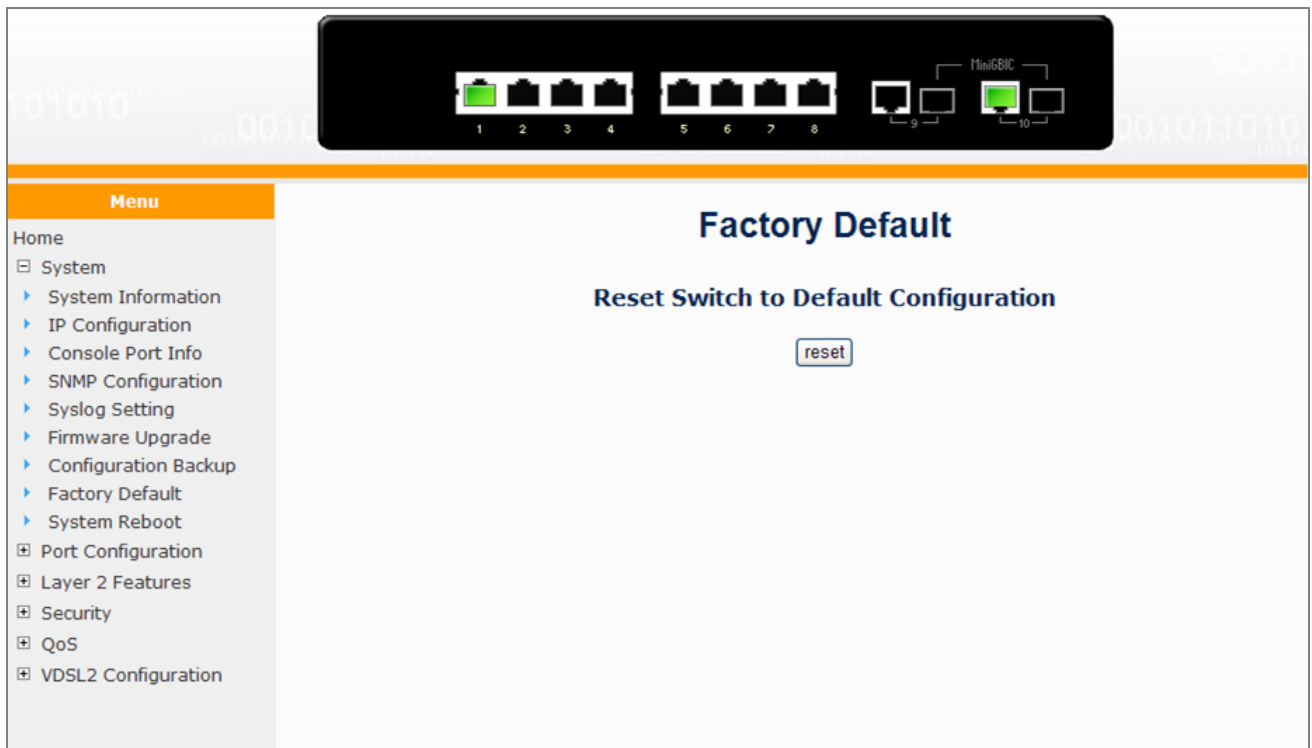


Figure 4-2-22: Factory Default interface

4.2.9 System Reboot

Reboot the switch in software reset. Click  to reboot the system.

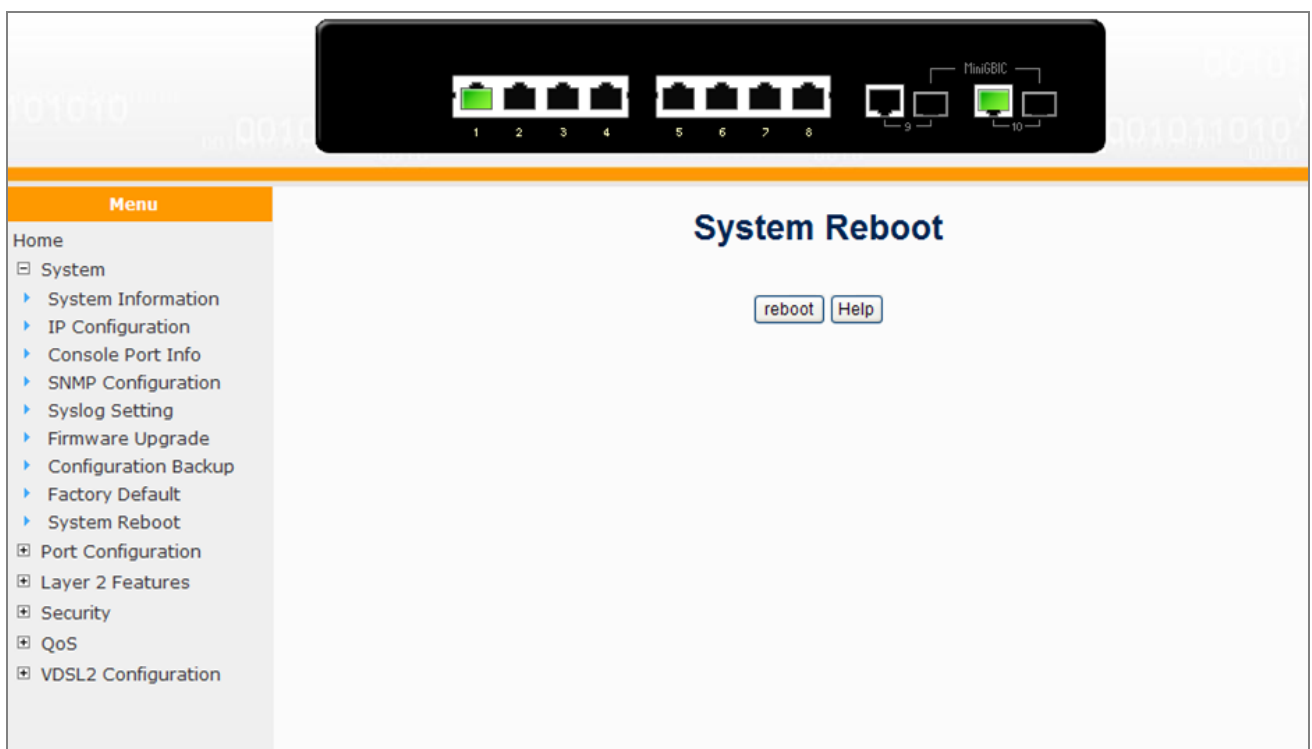


Figure 4-2-23: System Reboot interface

4.3 Port Configuration

Use the Port Configuration Menu to display or configure the Managed Switch's ports. This section has the following items:

- **Port Control** Configures port connection settings
- **Port Status** Display the current Port link status and speed etc.
- **Port Statistics** Lists Ethernet and RMON port statistics
- **Port Sniffer** Sets the source and target ports for mirroring
- **Protected Port** Configures Protected Ports and groups

4.3.1 Port Control

In Port control you can configure the settings of each port to control the connection parameters, and the status of each port is listed beneath.

The screenshot shows the 'Port Control' interface. At the top, there's a title 'Port Control'. Below it is a table with columns: Port, State, Negotiation, Speed, Duplex, Flow Control, Rate Control (Unit: 128Kbps) with sub-columns Ingress and Egress, Security, BSF, and Jumbo Frame. The first column 'Port' has a scroll bar with options Port1, Port2, Port3, and Port4. The 'State' column has a dropdown menu currently set to 'Enable'. The 'Negotiation' column has a dropdown menu set to 'Auto'. The 'Speed' column has a dropdown menu set to '1000'. The 'Duplex' column has a dropdown menu set to 'Full'. The 'Flow Control' column has a dropdown menu set to 'Enable'. The 'Rate Control' columns have input fields set to '0'. The 'Security' column has a checkbox that is unchecked. The 'BSF' column has a dropdown menu set to 'Enable'. The 'Jumbo Frame' column has a dropdown menu set to 'Enable'. Below the table is an 'Apply' button. At the bottom, there's another table with the same columns, but the 'Port' column is empty.

Figure 4-3-1: Port Control interface

The page includes the following fields:

Object	Description
Port:	Use the scroll bar and click on the port number to choose the port to be configured.
State:	Current port state. The port can be set to disable or enable mode. If the port state is set as 'Disable', it will not receive or transmit any packet. The item is only for Gigabit ports of the Managed Switch.
Negotiation:	Auto and Force . Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to set the speed and duplex mode manually.
Speed:	The item is only for Gigabit ports of the Managed Switch. It is available for selecting when the Negotiation column is set as Force. When

	the Negotiation column is set as Auto, this column is read-only.
Duplex:	The item is only for Gigabit ports of the Managed Switch. It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
Flow Control:	Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
Rate Control: (Unit: 128KBbps)	The item is only for Gigabit ports of the Managed Switch. Supports by-port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate at 1Mbps and ingress rate at 500Kbps. Device will perform flow control or backpressure to confine the ingress rate to meet the specified rate. ■ Ingress: Type the port effective ingress rate. The valid range is 0 ~ 8000. The unit is 128K. 0: disable rate control. 1 ~ 8000: valid rate value ■ Egress: Type the port effective egress rate. The valid range is 0 ~ 8000. The unit is 128K. 0: disable rate control. 1 ~ 8000: valid rate value.
Security:	A port in security mode will be "locked" without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings, then click Apply button to change on this page.
BSF:	User can disable/Enable port broadcast storm filtering option by port. The filter mode and filter packets type can be select in Switch Setting > Misc Config page.
Jumbo Frame:	User can disable/Enable port jumbo frame option by port. When port jumbo frame is enable, the port forward jumbo frame packet.



The Managed Switch support up to **9Kbytes** jumbo frame forwarding.

4.3.2 Port Status

This page displays current port configurations and operating status - it is a ports' configurations summary table. Via the summary table, you can know status of each port clear at a glance, like Port Link Up/Link Down status, negotiation, Link Speed, Rate Control, Duplex mode and Flow Control.

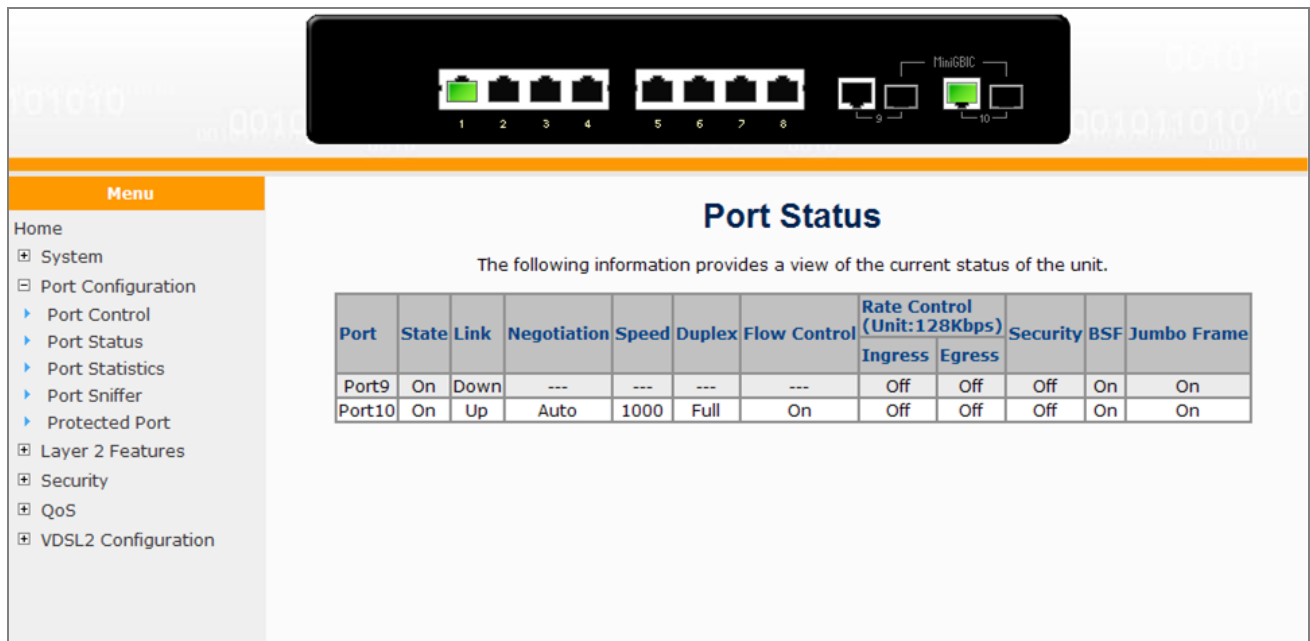


Figure 4-3-2: Port Status interface

4.3.3 Port Statistics

The following chart provides the current statistic information which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

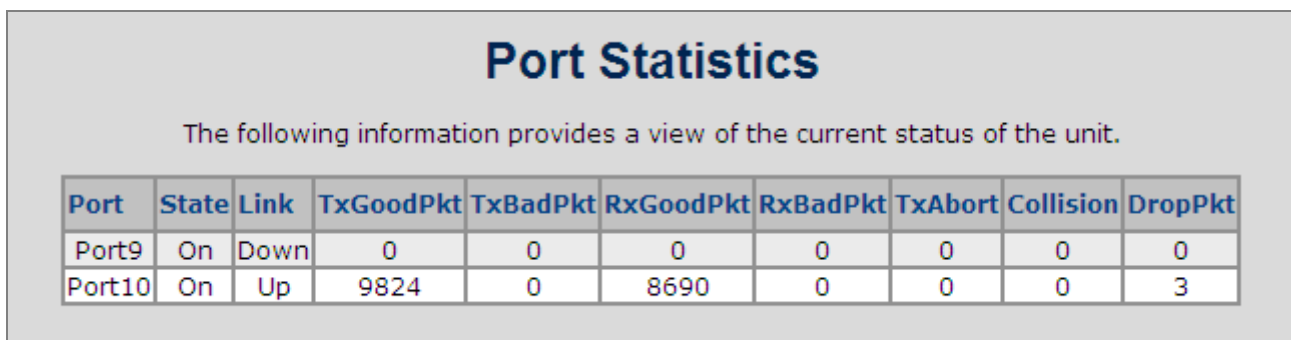


Figure 4-3-3: Port Statistics interface

The page includes the following fields:

Object	Description
Port:	The port number.

State:	It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
Link:	The status of linking—'Up' or 'Down'.
Tx Good Packet:	The counts of transmitting good packets via this port.
Tx Bad Packet:	The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
Rx Good Packet:	The counts of receiving good packets via this port.
Rx Bad Packet:	The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
Tx Abort Packet:	The aborted packet while transmitting.
Packet Collision:	The counts of collision packet.
Packet Dropped:	The counts of dropped packet.

4.3.4 Port Sniffer

The Port Sniffer (mirroring) is a method for monitor traffic in switched networks. Traffic through a port can be monitored by one specific port. That is, traffic goes in or out a monitored port will be duplicated into sniffer port.

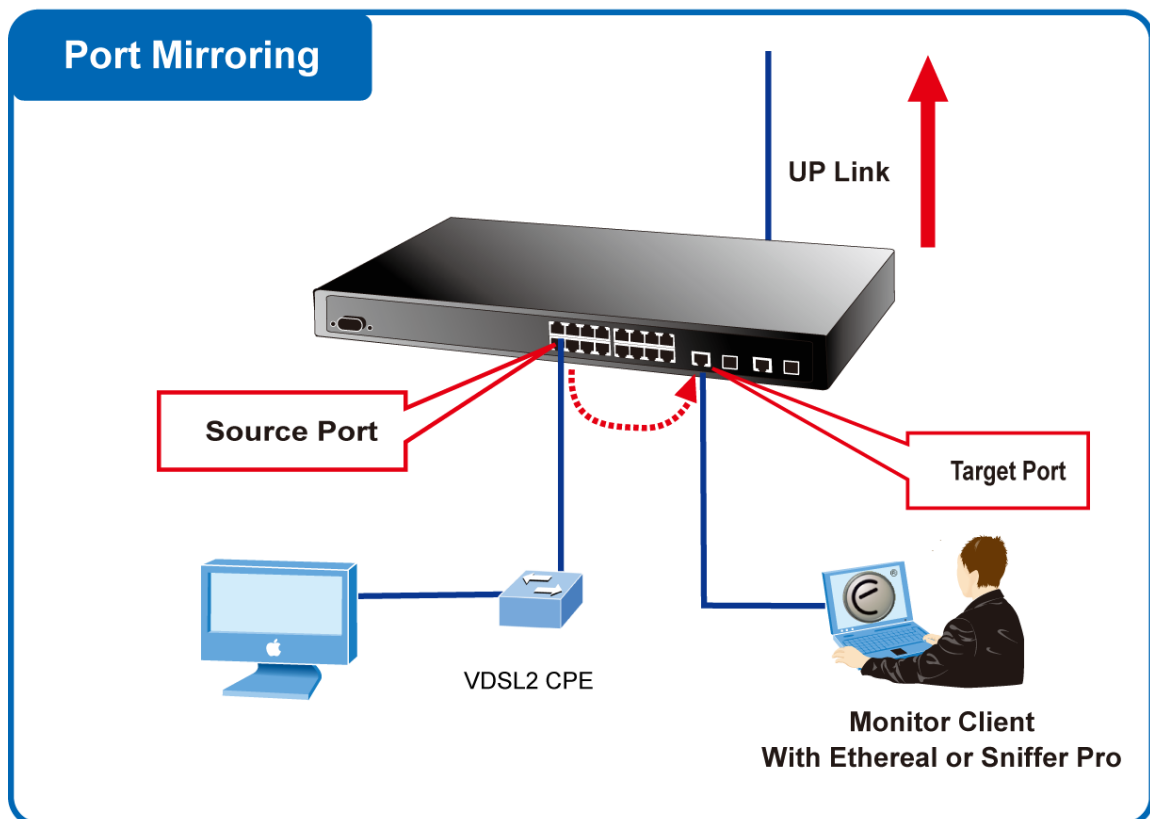


Figure 4-3-4: Port Mirror application

Configuring the port mirroring by assigning a source port from which to copy all packets and a destination port where those

packets will be sent.

Port Sniffer

Sniffer Type: BOTH

Analysis Port: Port1

Port	Monitor
Port1	☐
Port2	☒
Port3	☐
Port4	☐
Port5	☐
Port6	☐
Port7	☐
Port8	☐
Port9	☐
Port10	☐

Apply

Default

Help

Figure 4-3-5: Port Sniffer interface

The page includes the following fields:

Object	Description
Sniffer Type:	Select a sniffer mode: • DISABLE • RX • TT • BOTH
Analysis (Monitoring) Port:	It means Analysis port can be used to see the traffic on another port you want to monitor. You can connect Analysis port to LAN analyzer or netxray.
Monitored Port:	The port you want to monitor. The monitor port traffic will be copied to Analysis port. You can select one monitor ports in the switch. User can choose which port that they want to monitor in only one sniffer type.



- 1

When the Mirror Mode set to **RX** or **TX** and the **Analysis Port** be selected, the packets to and from the **Analysis Port** will not be transmitted. The Analysis Port will accept only COPIED packets from the **Monitored Port**.
- 2

If you want to disable the function, you must select monitor port to none.

4.3.5 Protect Port

There are two protected port groups; ports in different groups can't communicate.

In the same group, protected ports can't communicate with each other, but can communicate with unprotected ports.

Unprotected ports can communicate with any ports, including protected ports.

Portected Port Setting

Port ID	Protected	Group1	Group2
Port1	☐	☒	☐
Port2	☐	☒	☐
Port3	☐	☒	☐
Port4	☐	☒	☐
Port5	☐	☒	☐
Port6	☐	☒	☐
Port7	☐	☒	☐
Port8	☐	☒	☐
Port9	☐	☒	☐
Port10	☐	☒	☐

Figure 4-3-6: Protected Port Setting Web interface

The page includes the following fields:

Object	Description
Port ID	Identify the Managed Switch interface.
Protected	Enable the Protected function on the selected port. If the check box is not shown as ☒ , then this port a unprotected port and it can communicate with any ports - including protected ports
Group 1	Set the protected port to be Group 1 member.
Group 2	Set the protected port to be Group 2 member.



Usually, set the **Uplink port** or the Port is connected to Core switch or router to be the **Un-protected port**.

4.4 VLAN configuration

4.4.1 VLAN Overview

A **Virtual Local Area Network (VLAN)** is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.



1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

The Managed Switch supports **IEEE 802.1Q (tagged-based)** and **Port-Base VLAN** setting in web management page. In the default configuration, VLAN support is “**802.1Q**”.

■ Port-based VLAN

Port-based VLAN limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLAN, NIC do not need to be able to identify 802.1Q tags in packet headers. NIC send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

■ IEEE 802.1Q VLANs

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

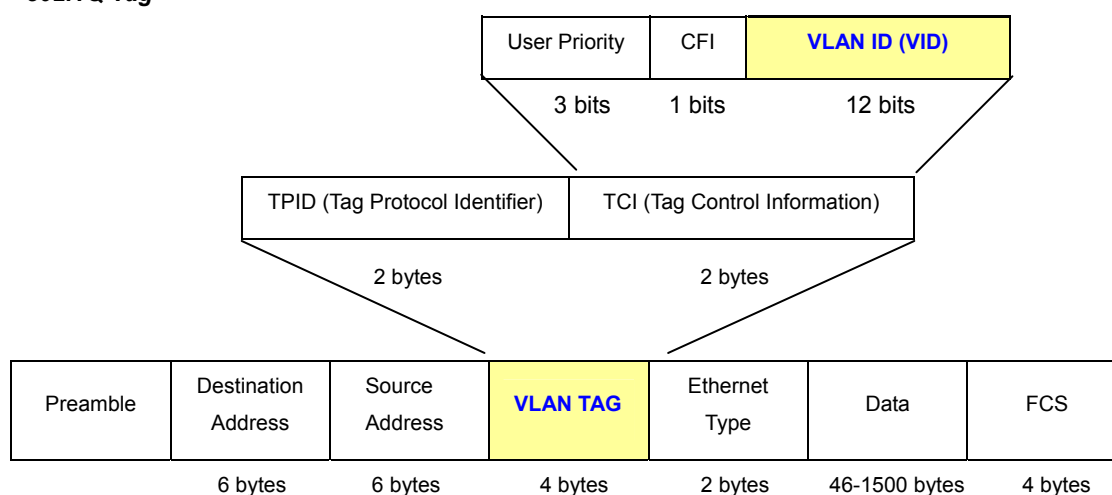
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

■ 802.1Q VLAN Tags

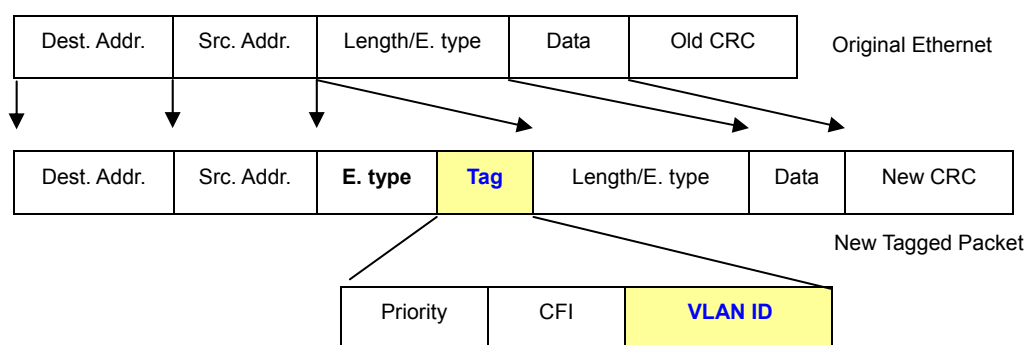
The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the Ether Type field. When a packet's Ether Type field is equal to **0x8100**, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag**■ Port VLAN ID**

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

■ Default VLANs

The Switch initially configures one VLAN, VID = 1, called **"default."** The factory default setting assigns all ports on the Switch to the **"default."** As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

■ VLAN and Link aggregation Groups

In order to use VLAN segmentation in conjunction with port link aggregation groups, you can first set the port link aggregation group(s), and then you may configure VLAN settings. If you wish to change the port link aggregation grouping with VLAN already in place, you will not need to reconfigure the VLAN settings after changing the port link aggregation group settings. VLAN settings will automatically change in conjunction with the change of the port link aggregation group settings.

4.4.2 Static VLAN Configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

The Managed Switch supports **Port-based** and **802.1Q (Tagged-based)** VLAN in web management page. In the default configuration, VLAN support is "802.1Q".

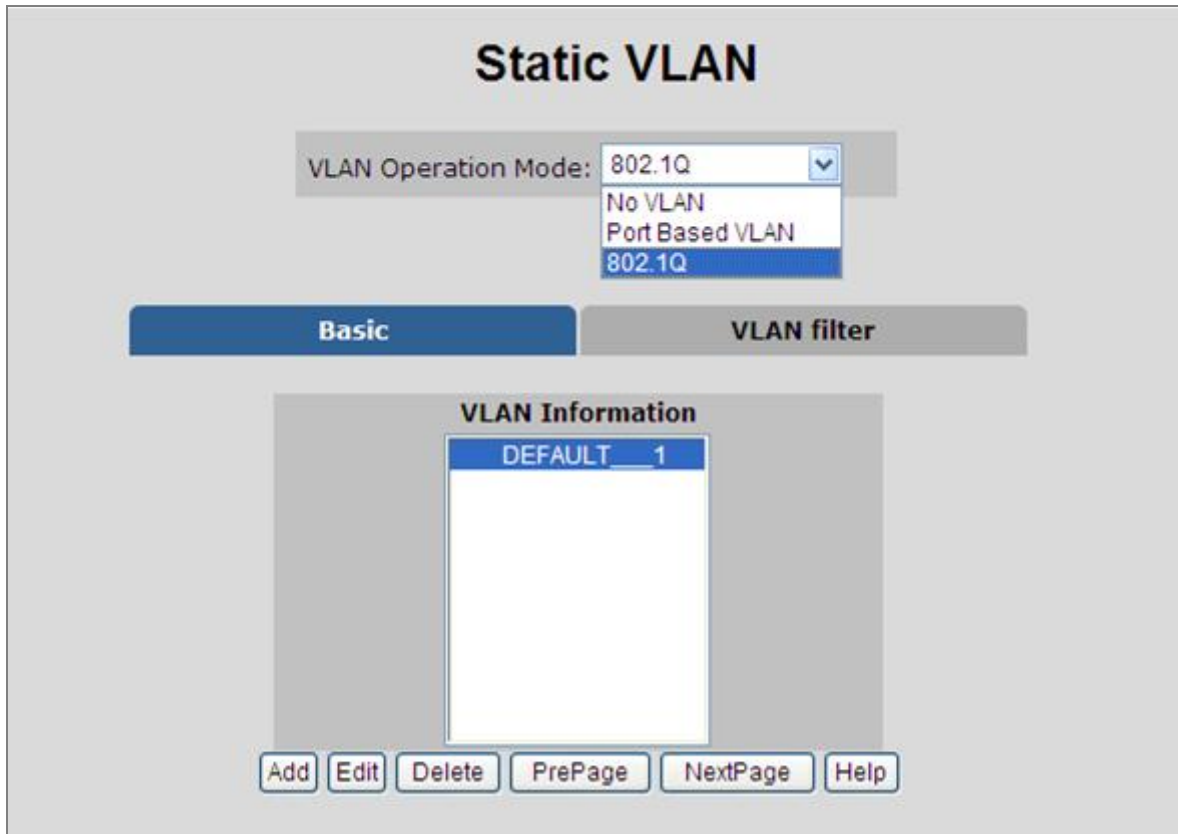


Figure 4-4-1: Static VLAN interface



- 1 No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
- 2 The Switch supports **Port-based VLAN** and **IEEE 802.1Q VLAN**. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

4.4.3 Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLANs, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

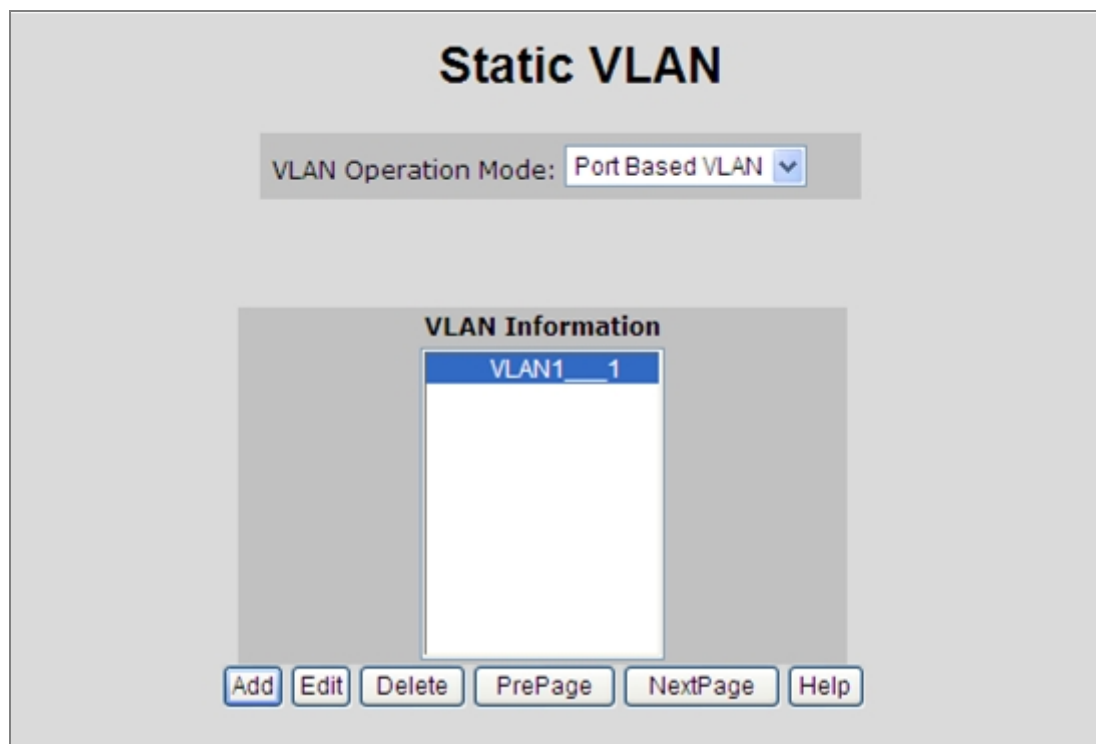


Figure 4-4-2: Port-based VLAN interface

■ Create a VLAN and add member ports to it

1. Click the hyperlink "**VLAN**" \ "**Static VLAN**" to enter the VLAN configuration interface.
2. Select "**Port Based VLAN**" at the VLAN Operation Mode, to enable the port-based VLAN function.
3. Click "**Add**" to create a new VLAN group. Then the following **Figure 4-4-3** appears.
4. Type a name and Group ID for the new VLAN, the available range is **2-4094**.
5. From the Available ports box, select ports to add to the Managed Switch and click "**Add**".
6. Click **Apply**.
7. You will see the VLAN Group displays.
8. If the port-based VLAN groups list over one page, please click "**Next Page**" to view other VLAN groups on other page.
9. Use "**Delete**" button to delete unwanted port-based VLAN groups
10. Use "**Edit**" button to modify existing port-based VLAN groups.

By adding ports to the VLAN you have created one port-based VLAN group completely.

Static VLAN

VLAN Operation Mode: Port Based VLAN

VLAN Name:

VLAN-1

Group ID:

1

Port5
Port6
Port7
Port8
Port9
Port10

Add >>

<< Remove

Port1
Port2
Port3
Port4

☐ CPU Port

Apply

Help

Figure 4-4-3: Static VLAN interface

The page includes the following fields:

Object	Description
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 16 alphanumeric characters long, including blanks.
Group ID	You can configure the ID number of the VLAN by this item. This field is used to add VLANs one at a time. The VLAN group ID and available range is 2-4094 .
Port	Indicate port 1 to port 10.
Member	Add Defines the interface as a Port-Based member of a VLAN.
	Remove Forbidden ports are not included in the VLAN.

All unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

72

4.4.4 802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create and delete Tag-based VLAN. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can't be deleting.

Understand nomenclature of the Switch

■ IEEE 802.1Q Tagged and Untagged

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

- Tagged** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- Untagged** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

4.4.4.1 VLAN Group Configuration

■ VLAN Group Configuration

The image shows a web-based configuration interface for Static VLAN. At the top, the title "Static VLAN" is centered. Below it, a dropdown menu for "VLAN Operation Mode" is set to "802.1Q". There are two tabs: "Basic" (active) and "VLAN filter". Under the "Basic" tab, there is a section titled "VLAN Information" containing a table with one row: "DEFAULT" and "1". Below the table are six buttons: "Add", "Edit", "Delete", "PrePage", "NextPage", and "Help".

VLAN Information	
DEFAULT	1

Figure 4-4-4: VLAN Group Configuration interface

1. Click the hyperlink "**VLAN**" \ "**Static VLAN**" to enter the VLAN configuration interface.
2. Select "**802.1Q**" at the **VLAN Operation Mode**, to enable the 802.1Q VLAN function.
3. Click **Add** to create a new VLAN group or Edit to management exist VLAN groups. Then the VLAN Group column appears.
4. Input a VLAN group ID and available range is 2-4094.

Static VLAN

VLAN Operation Mode: 802.1Q ▼

VLAN Group
VLAN Filter

VLAN Name:

VID:

Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10	Add >> << Remove	
---	--	--

☐ **CPU Port**

Apply
Help

Figure 4-4-5: VLAN Group Configuration interface

5. Select specific port as member port and the screen in Figure 4-4-6 appears.
6. After setup completed, please press "**Apply**" button to take effect.
7. Please press "**Back**" for return to VLAN configuration screen to add other VLAN group, the screen in Figure 4-33 appears.
8. If there are many groups that over the limit of one page, you can click **Next** to view other VLAN groups.
9. Use **Delete** button to delete unwanted VLAN.
10. Use **Edit** button to modify existing VLAN group.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Name: DEFAULT

VLAN ID: 1

UnTag Member

Port1	Untag	Port2	Untag
Port3	Untag	Port4	Untag
Port5	Untag	Port6	Untag
Port7	Untag	Port8	Untag
Port9	Untag	Port10	Untag

Apply

Figure 4-4-6: 802.1Q VLAN Setting Web Page screen

The page includes the following fields:

Object	Description
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 16 alphanumeric characters long, including blanks.
VLAN ID	You can configure the ID number of the VLAN by this item. This field is used to add VLANs one at a time. The VLAN group ID and available range is 2-4094 .
Port	Indicate port 1 to port 10.
UnTag Member	Untag Packets forwarded by the interface are untagged.
	Tag Defines the interface as a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.



Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can't be deleted.

4.4.4.2 VLAN Filter

■ 802.1Q VLAN Port Configuration

This page is used for configuring the Switch port VLAN. The VLAN per Port Configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (**PVID**) is configured on the VLAN Port Configuration page. All untagged packets arriving to the device are tagged by the ports PVID.

This section provides 802.1Q Ingress Filter of each port from the Switch, the screen in [Figure 4-4-7](#) appears.

Static VLAN

VLAN Operation Mode: 802.1Q

Basic

VLAN filters

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)
Ingress Filtering Rule 2
(Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1 Port2 Port3 Port4	1	Enable	Disable

ApplyDefaultHelp

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port2	1	ENABLE	DISABLE

Figure 4-4-7: 802.1Q Ingress filter interface

The page includes the following fields:

Object	Description
NO	Indicate port 1 to port 10.
PVID	Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. The switch each port allows user to set one VLAN ID, the range is 1~255, default

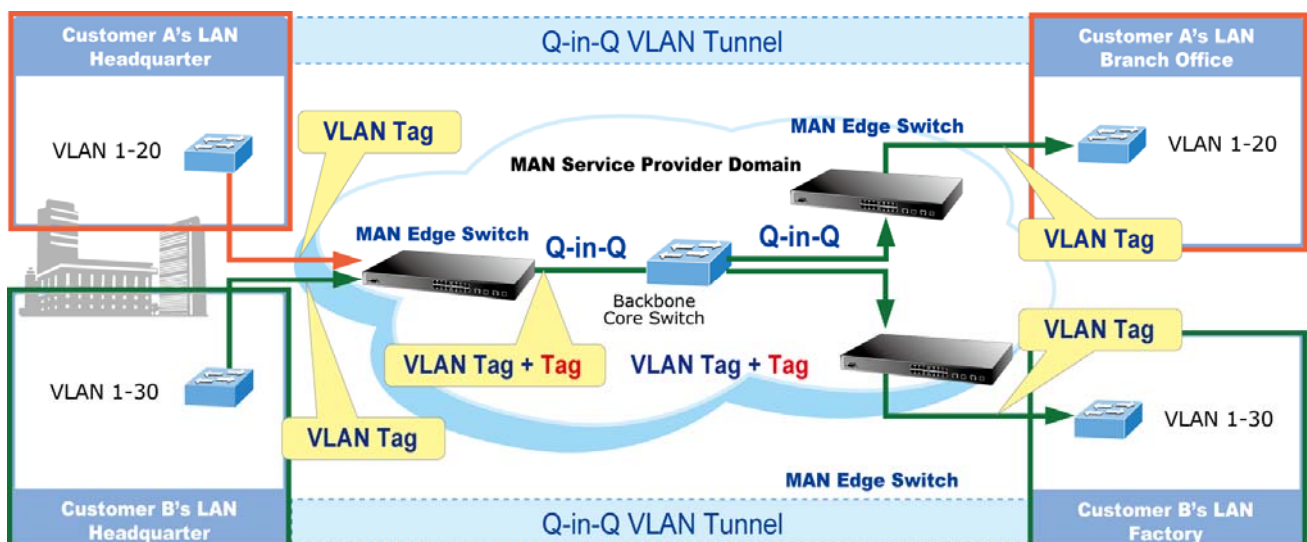
	VLAN ID is 1.
	The VLAN ID must be the same as the VLAN ID that the port belongs to VLAN group, or the untagged traffic will be dropped.
Ingress Filtering 1	Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN. Enable: Forward only packets with VID matching this port's configured VID. Disable: Disable Ingress filter function.
Ingress Filtering 2	Drop untagged frame. Disable: Acceptable all Packet. Enable: Only packet with match VLAN ID can be permission to go through the port.
Apply button	Press the button to save configurations.

4.4.5 Q-in-Q VLAN

■ IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The Managed Switch supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote customer VLANs through a common MAN space without interfering with the VLAN tags. All tags use Ether Type **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

4.4.5.1 Q-in-Q Port Setting

The QinQ VLAN \ **QinQ Port Setting** screen in [Figure 4-4-8](#) appears.

QinQ VLAN

QinQ Port Setting

QinQ Tunnel Setting

QinQ

Enable

QinQ Tpid

8100

Port	QinQ	QinQ Uplink
Port1	☐	☐
Port2	☐	☐
Port3	☐	☐
Port4	☐	☐
Port5	☐	☐
Port6	☐	☐
Port7	☐	☐
Port8	☐	☐
Port9	☐	☐
Port10	☐	☐

Figure 4-4-8: Q-in-Q Port Setting interface

The page includes the following fields:

Object	Description
QinQ	Enable: Sets the Managed Switch to QinQ mode, and allows the QinQ tunnel port to be configured.
	Disable: The Managed Switch operates in its normal VLAN mode.
	The default is for the Managed Switch to function in Disable mode.
QinQ TPID	The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel access port. • 802.1Q Tag: 8100 • vMAN Tag: 88A8 Default: 802.1Q Tag.
Port QinQ	Check: Sets the Port to QinQ mode. Or the port operates in its normal VLAN mode. Default: Un-check.
QinQ Uplink	Check: Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network.
	Cancel: Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.

4.4.5.2 Q-in-Q Tunnel Setting

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.

Using the QinQ feature, service providers can use a single VLAN to support customers who have multiple VLANs.

Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using QinQ expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support QinQ is called a QinQ user-port. A port configured to support QinQ Uplink is called a QinQ uplink-port.

QinQ VLAN	
QinQ Tunnel Setting	
Tunnel ID	Tunnel1
Tunnel VID	0
	<< Get << Add << Remove >> Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port9
Apply Delete Help	

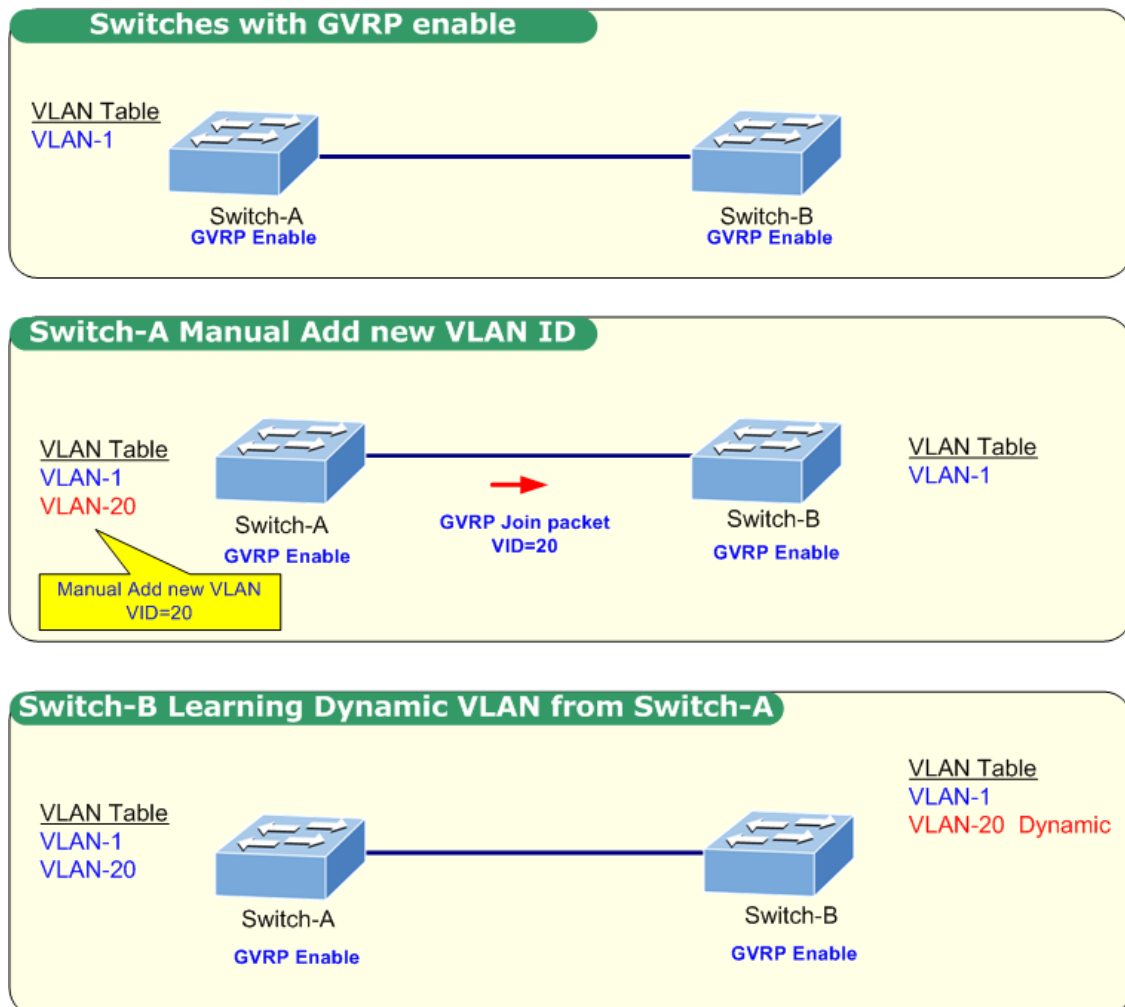
Figure 4-4-9: Q-in-Q Tunnel Setting interface

■ To configure QinQ Port

1. Enable global QinQ function: select **QinQ** enable "**Enable**".
2. Fill QinQ Tpid.
3. Enable port QinQ function: select QinQ checkbox for special port.
4. Enable port QinQ Uplink function: select QinQ Uplink checkbox for special port.

4.4.6 GVRP VLAN

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.



4.4.6.1 GVRP Setting

To configure GVRP

Enable global GVRP function: select GVRP enable "Enable".

Enable port GVRP function: select GVRP checkbox for special port.

GVRP Configuration

GVRP Setting

GVRP Table

GVRP

Disable

Port	GVRP
Port1	☐
Port2	☐
Port3	☐
Port4	☐
Port5	☐
Port6	☐
Port7	☐
Port8	☐
Port9	☐
Port10	☐

Apply

Default

Help

Figure 4-4-10: GVRP Configuration Web interface

The page includes the following fields:

Object	Description
GVRP	Enable global GVRP function
Port	Indicate port 1 to port 10.
Port GVRP	Enable selected port GVRP function

4.4.6.2 GVRP Table

The GVRP Table can be used to display dynamic VLANs from being learned via GVRP.

GVRP Configuration		
GVRP Setting		GVRP Table
No	VLAN ID	Port members
1	2	9
2	3	9
3	4	9
4	5	9
5	6	9
6	7	9
7	8	9
8	9	9
9	10	9
10	11	9
11	12	9
12	13	9
13	14	9
14	15	9
15	16	9
16	17	9
17	18	9
18	19	9
19	20	9

Figure 4-4-11: GVRP Table Web interface

The page includes the following fields:

Object	Description
VLAN ID	Display the learned VLANs via GVRP protocol on GVRP enabled ports. The Managed Switch allows displaying up to 128 dynamic VLAN entries.
Port Members	Identify the GVRP enabled port that dynamic VLAN is learned from.

4.5 Trunking

Port Trunking (also called “Link Aggregation”) is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. The Managed Switch supports two types of port trunk technology:

- Static Trunk
- LACP

The **Link Aggregation Control Protocol (LACP)** provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires Full-duplex mode**, more detail information refers to IEEE 802.3ad.

4.5.1 Aggregator setting

This section provides Port Trunk-Aggregator Setting of each port from the Managed Switch, the screen in [Figure 4-6-1](#) appears.

Trunking

Aggregator Setting

Aggregator Information

State Activity

LACP	System Priority
☒	32768

Group ID	1	<< Get
LACP	Enable	
Work Ports	2	
Port9 Port10	<< Add << Remove>>	Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8

Apply

Delete

Help

Figure 4-5-1: Port Trunk—Aggregator setting interface (two ports are added to the left field with LACP enabled)

The page includes the following fields:

Object	Description
System Priority:	A value which is used to identify the active LACP. The Managed Switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.
Group ID:	There are 13 trunk groups to be selected. Assign the " Group ID " to the trunk group.
LACP:	■ Enabled, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. ■ Disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.
Work ports:	This column field allows the user to type in the total number of active port up to four. With LACP s tatic trunk group , e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a static trunk group (non-LACP), the number of work ports must equal the total number of group member ports.



Please notice that a trunk group, including member ports split between two switches, **has to enable the LACP function of the two switches**.

4.5.2 Aggregator Information

When you had setup the LACP aggregator, you will see relation information in here.

■ LACP disabled

Having set up the aggregator setting with LACP disabled, you will see the local static trunk group information on the tab of **Aggregator Information**.

Trunking

Aggregator Setting

Aggregator Information

State Activity

LACP

☐

System Priority

32768

Group ID

1

<< Get

LACP

Disable

Work Ports

2

Port9
Port10

<< Add <<
Remove>>

Port1
Port2
Port3
Port4
Port5
Port6
Port7
Port8

Apply

Delete

Help

Figure 4-5-2: Assigning 2 ports to a trunk group with LACP disabled

Trunking

Aggregator Setting

Aggregator Information

State Activity

The following information provides a view of LACP current status.

Static Trunking Group

Group Key

1

Port_No

9 10

Figure 4-5-3: Static Trunking Group information

The page includes the following fields:

Object	Description
Group Key:	This is a read-only column field that displays the trunk group ID.
Port Member:	This is a read-only column field that displays the members of this static trunk group.

87

■ LACP enabled

Having set up the aggregator setting with LACP enabled, you will see the trunking group information between two switches on the tab of **Aggregator Information**.

■ Switch 1 configuration

1. Set **System Priority** of the trunk group. The default is **32768**.
2. Select a **trunk group ID** by pull down the drop-down menu bar.
3. Enable **LACP**.
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.

The screenshot displays the 'Trunking' configuration window with three tabs: 'Aggregator Setting', 'Aggregator Information', and 'State Activity'. The 'Aggregator Information' tab is active. It contains a table for LACP settings with 'LACP' checked and 'System Priority' set to 32768. Below this is a section for Group ID (1), LACP (Enable), and Work Ports (2). A list of ports (Port1 to Port10) is shown on the right, with Port1 and Port2 selected. Buttons for '<< Add <<', 'Remove>>', '<< Get', 'Apply', 'Delete', and 'Help' are visible.

Trunking			
Aggregator Setting		Aggregator Information	State Activity
LACP	System Priority		
☒	32768		
Group ID	1 ▼	<< Get	
LACP	Enable ▼		
Work Ports	2		
Port1 Port2	<< Add << Remove>>	Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10	
Apply Delete Help			

Figure 4-5-4: Aggregation Information of **Switch 1**

5. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.

■ Switch 2 configuration

6. Set **System Priority** of the trunk group. For example: 1.
7. Select a **trunk group ID** by pull down the drop-down menu bar.
8. Enable LACP.
9. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.

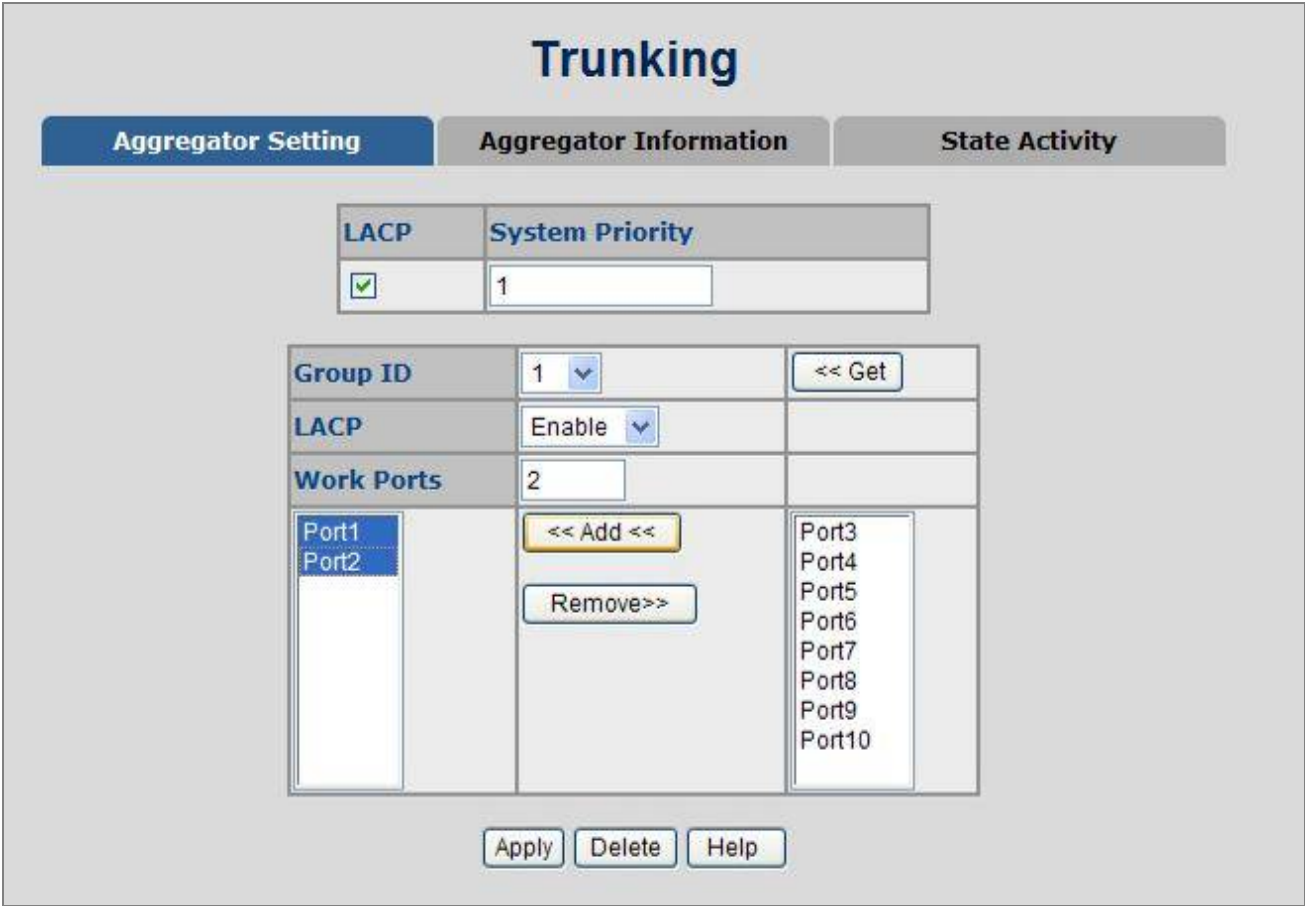


Figure 4-5-5: Switch 2 configuration interface

10. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.



Figure 4-5-6: Switch 1 Aggregator Information

4.5.3 State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state label. When you remove the tick mark of the port and click **Apply**, the port state activity will change to **Passive**.

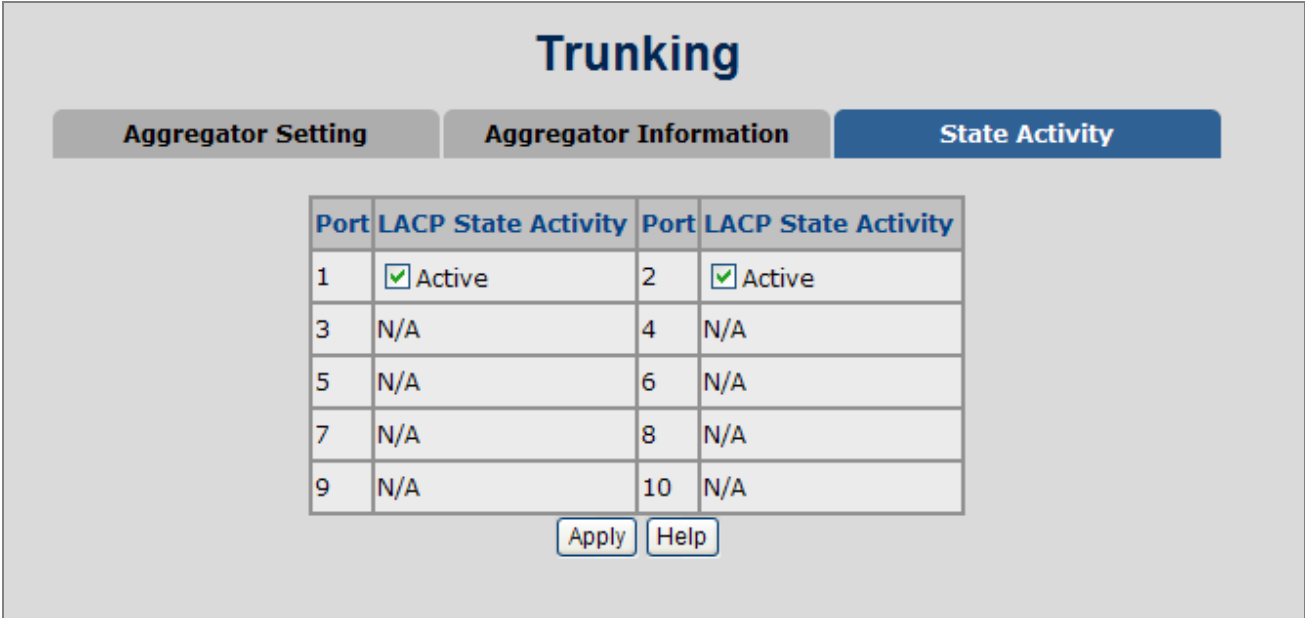


Figure 4-5-7: State Activity of Switch 1

The page includes the following fields:

Object	Description
Active:	The port automatically sends LACP protocol packets.
Passive:	The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.



A link having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.

4.6 Forwarding and Filtering

The frames of Ethernet Packets contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frames with the corresponding SMAC address have been seen after a configurable age time.

4.6.1 Dynamic MAC Table

Entries in the MAC Table are shown on this page. The Dynamic MAC Table contains up to **8192** entries, and is sorted first by VLAN ID, then by MAC address. You can view all of the dynamic MAC addresses learned by the listed port.

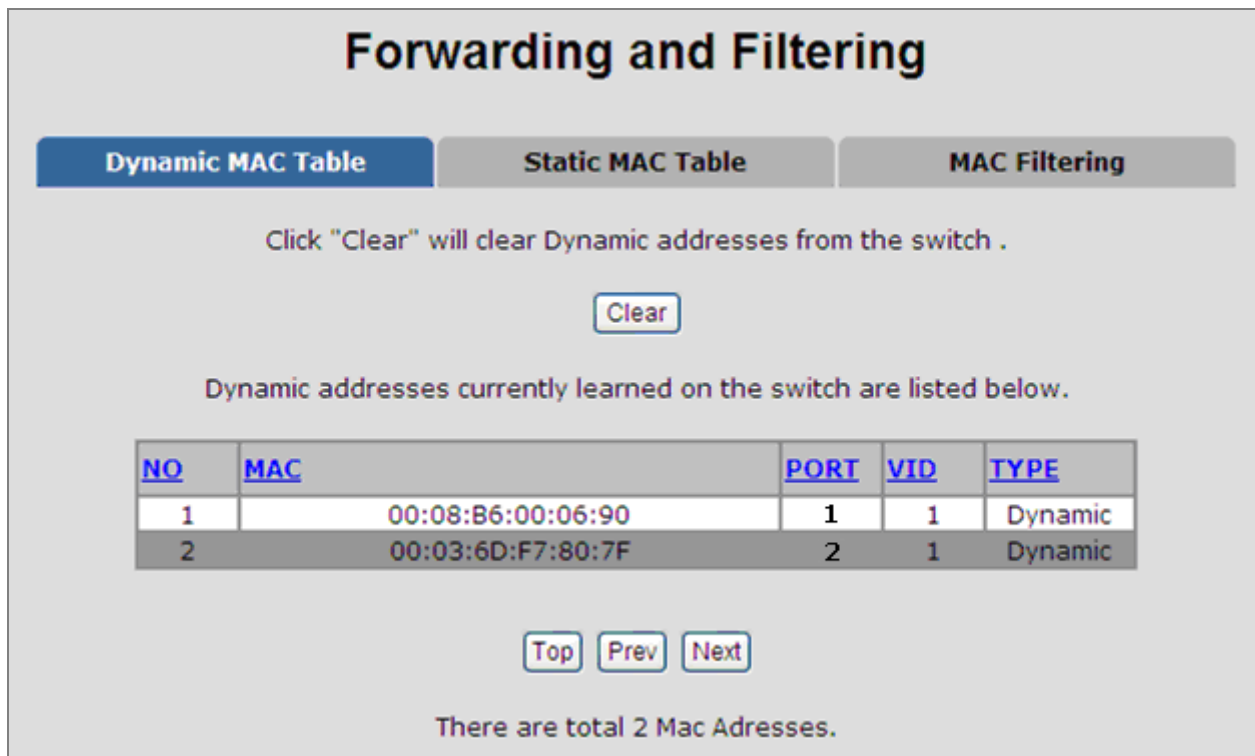


Figure 4-6-1: Dynamic MAC Address interface

MAC Table Columns

Object	Description
• NO	The MAC address index entry.
• MAC	The MAC address of the entry.
• PORT	The ports that are members of the entry.
• VID	The VLAN ID of the entry.
• Type	Indicates whether the entry is a static or dynamic entry.

Click "**Clear**" to clear the dynamic MAC addresses information of the current port shown on the screen.

4.6.2 Static MAC Table

You can add a static MAC address that remains in the switch's address table regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. Via this interface, you can add / delete a static MAC address.

■ **Add the Static MAC Address**

You can add static MAC address in the switch MAC table here.

Forwarding and Filtering

Dynamic MAC Table

Static MAC Table

MAC Filtering

Dynamic addresses currently defined on the switch are listed below.
Click Add to add a new static entry to the address table.

MAC Address _____ PORT _____ VID _____

00:33:4F:11:22:33

1

1

MAC Address

00:33:4F:22:33:44

Port num

Port 2

VLAN ID

1

Add

Delete

Help

Figure 4-6-2: Static MAC Addresses interface

The page includes the following fields:

Object	Description
MAC Address:	Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
Port num.:	Pull down the selection menu to select the port number.
VLAN ID:	The VLAN ID for the entry.

92

4.6.3 MAC Filtering

By filtering MAC address, the switch can easily filter the pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address.

Forwarding and Filtering

Dynamic MAC Table

Static MAC Table

MAC Filtering

Specify a MAC address to filter.

00:36:4F:55:66:771

00:30:47:77:2B:FC1

MAC Address00:e0:3A:11:22:33

VLAN ID2

Add

Delete

Help

NO	MAC	SOURCE	VID	TYPE
1	00:36:4F:55:66:77	Filter	1	Static
2	00:30:47:77:2B:FC	Filter	1	Static

Figure 4-6-3: MAC Filtering interface

The page includes the following fields:

Object	Description
MAC Address:	Enter the MAC address that you want to filter.
VLAN ID:	The VLAN ID for the entry.

4.7 IGMP Snooping

4.7.1 Theory

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'querier'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

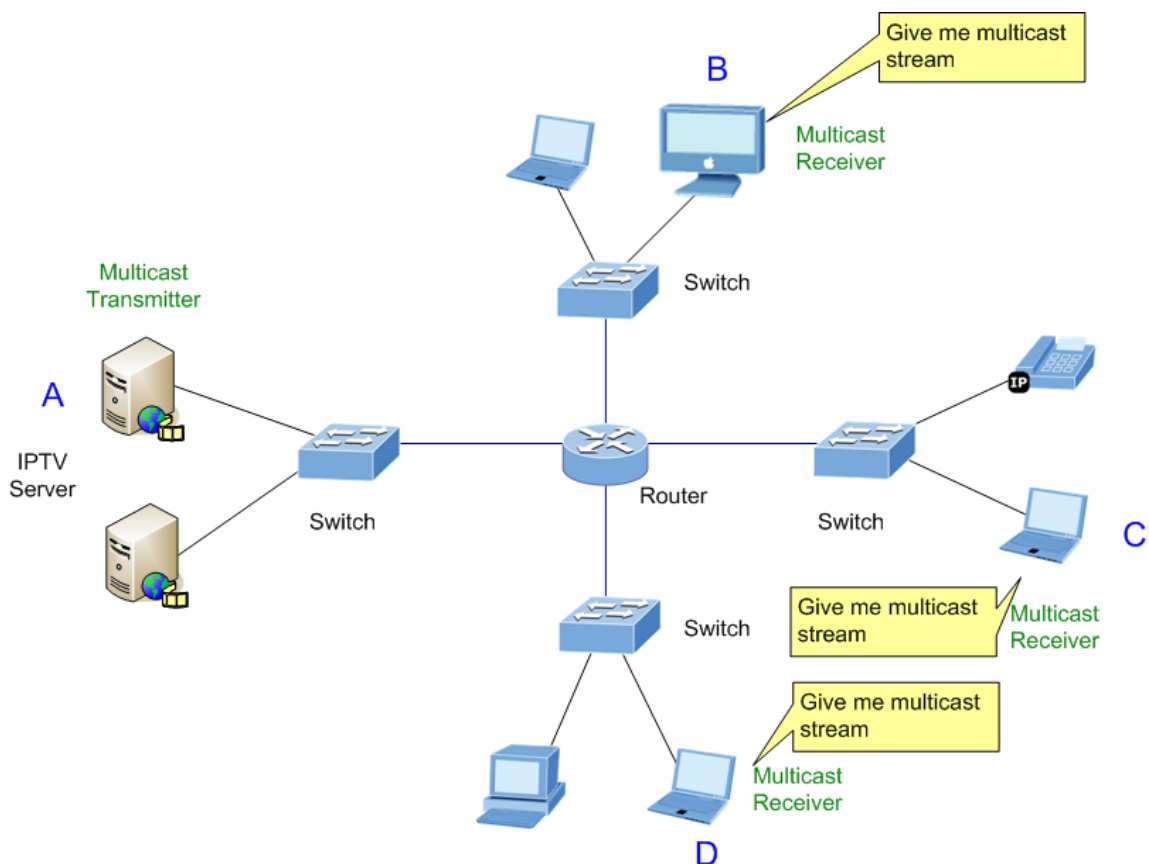


Figure 4-7-1: Multicast Service

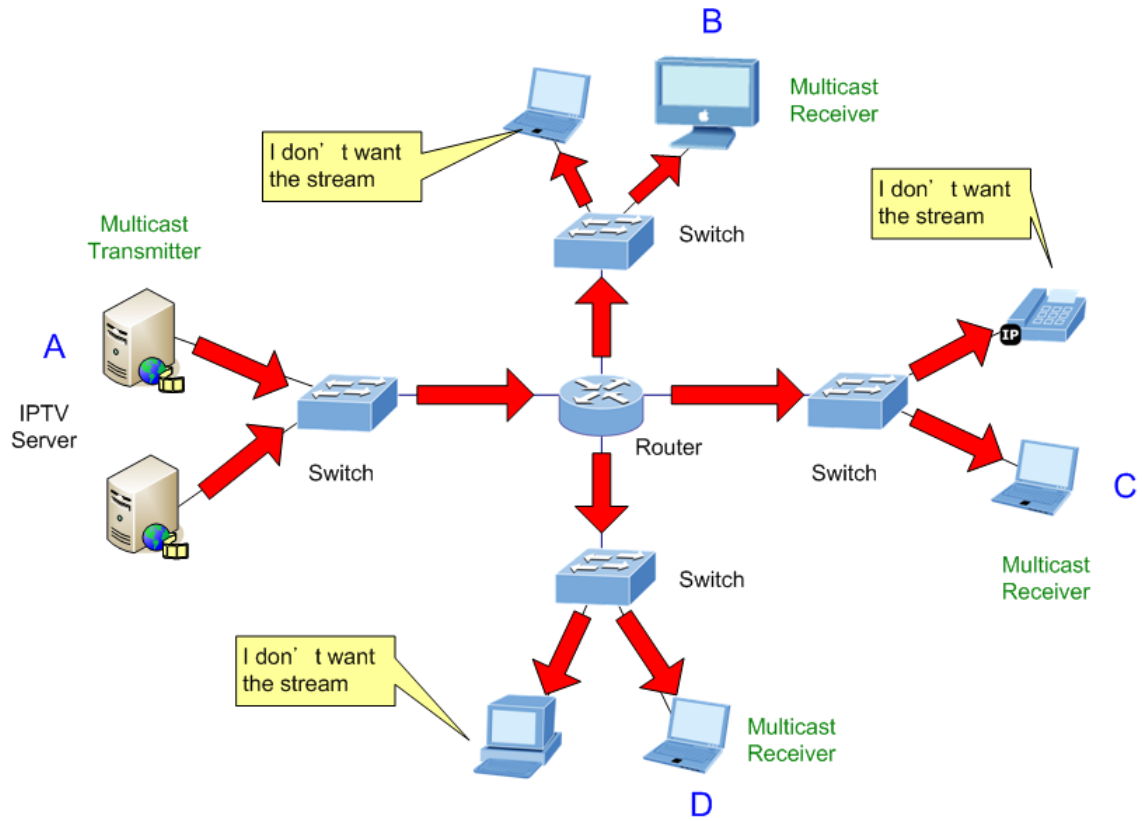


Figure 4-7-2: Multicast flooding

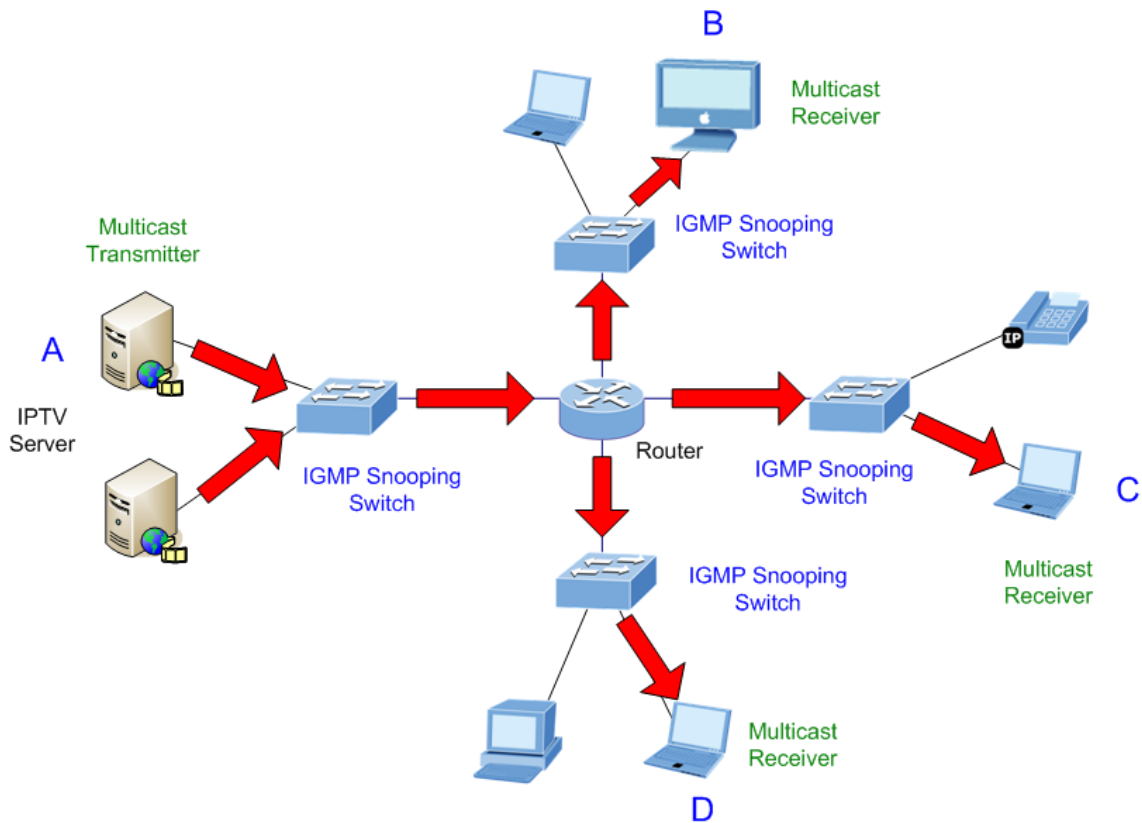


Figure 4-7-3: IGMP Snooping multicast stream control

IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0	8	16	31
Type	Response Time	Checksum	
Group Address (all zeros if this is a query).			

The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0).
0x11	Specific Group Membership Query (if Group Address is Present).
0x16	Membership Report (version 2).
0x17	Leave a Group (version 2).
0x12	Membership Report (version 1).

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

A host sends an IGMP **“report”** to join a group.

A host will never send a report when it wants to leave a group (for version 1).

A host will send a **“leave”** report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:

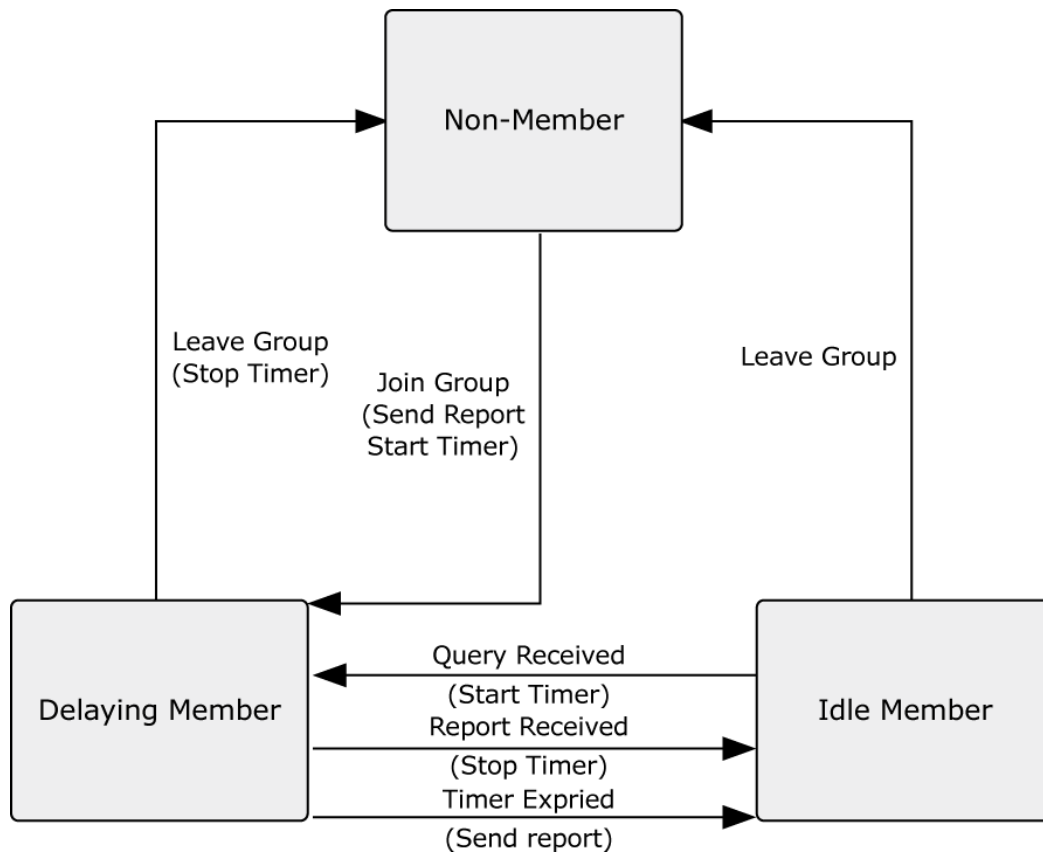


Figure 4-7-4: IGMP State Transitions

■ IGMP Querier

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router / switch on the LAN performing IP multicasting, one of these devices is elected “**querier**” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.



Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

4.7.2 IGMP Configuration

The Switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then the IGMP snooping information displays. IP multicast addresses range are from **224.0.0.0** through **239.255.255.255**.

IGMP Snooping

IGMP Protocol: Enable

IGMP fastleave: Enable

IGMP Querier: Enable

Multicast Group

Ip_Address	VID	MemberPort
239.255.255.250	1	*****g*****
224.000.000.251	1	*****g*****
224.000.000.252	1	*****g*****
224.000.001.024	1	*****g*****

Apply

Figure 4-7-5: IGMP Configuration interface

The page includes the following fields:

Object	Description
IGMP Protocol:	Enable or disable the IGMP protocol.
IGMP Fast leave:	Enable or disable Fast Leave on the port.
IGMP Querier:	Enable or disable the IGMP query function. The IGMP query information will be displayed in IGMP status section.

Fast Leave:



The Managed Switch can be configured to immediately delete a member port of a multicast service if a leave packet is received at that port and the fast leave function is enabled for the parent VLAN. This allows the Managed switch to remove a port from the multicast forwarding table without first having to send an IGMP group-specific query to that interface.

4.8 Spanning Tree Protocol

4.8.1 Theory

The Spanning Tree protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this Managed Switch include these versions:

- **STP – Spanning Tree Protocol (IEEE 802.1D)**
- **MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)**

STP - The Spanning Tree Protocol (STP) is a standardized method (**IEEE 802.1D**) for avoiding loops in switching networks. Enable STP to ensure that only one path at a time is active between any two nodes on the network.

MSTP - The Multiple Spanning Tree Protocol (MSTP) is a standardized method (**IEEE 802.1S**) for providing simple and full connectivity for frames assigned to any given VLAN throughout a Bridged Local Area Network comprising arbitrarily interconnected Bridges, each operating MSTP, STP, or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent **Multiple Spanning Tree Instance (MSTI)**, within **Multiple Spanning Tree (MST)** Regions composed of LANs and or MST Bridges. These Regions and the other Bridges and LANs are connected into a single **Common Spanning Tree (CST)**.

The **IEEE 802.1D Spanning Tree** Protocol and **IEEE 802.1s Multiple Spanning Tree** Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using **Bridge Protocol Data Units (BPDUs)**. Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch.
- The path cost to the root from the transmitting port.
- The port identifier of the transmitting port.

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the **root switch**.
- The shortest distance to the root switch is calculated for each switch.
- A **designated switch** is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists in one of the following five states:

- **Blocking** – the port is blocked from forwarding or receiving packets.
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state.
- **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets.
- **Forwarding** – the port is forwarding packets.
- **Disabled** – the port only responds to network management messages and must return to the blocking state first.

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking.
- From blocking to listening or to disabled.
- From listening to learning or to disabled.
- From learning to forwarding or to disabled.
- From forwarding to disabled.
- From disabled to blocking.

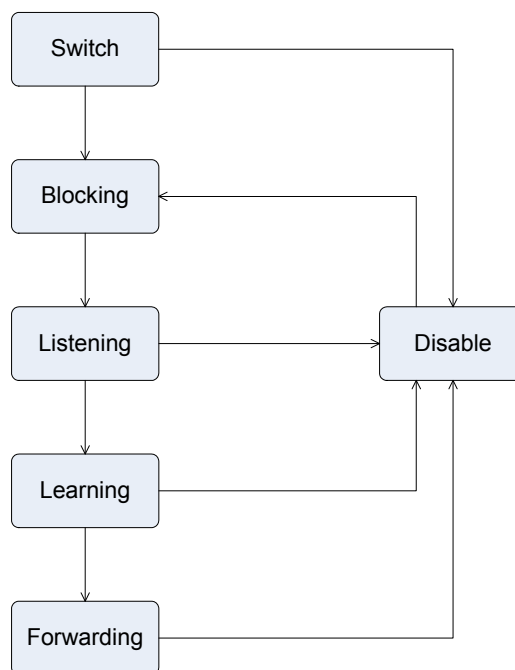


Figure 4-8-1: STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

4.8.2 Illustration of STP

A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.

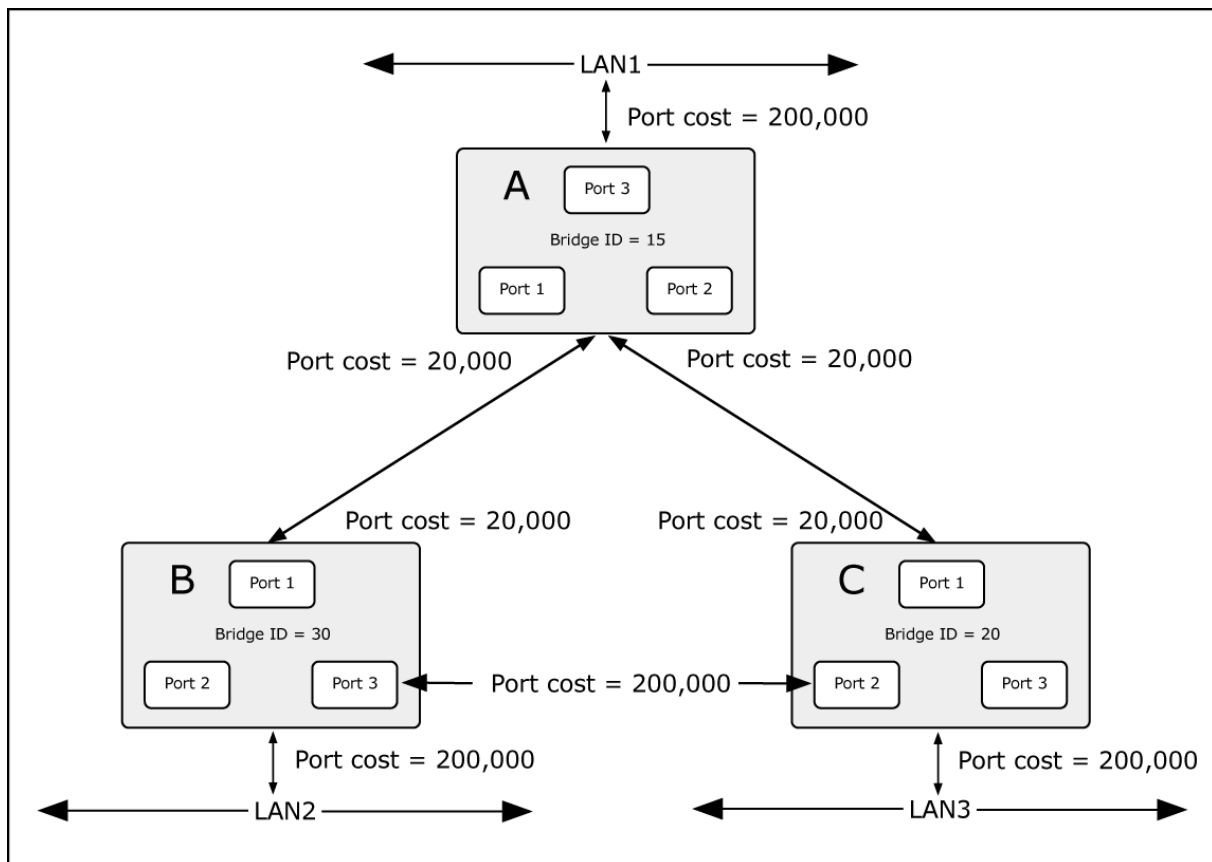


Figure 4-8-2: Before Applying the STA Rules

If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings.

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

In this example, only the default STP values are used.

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

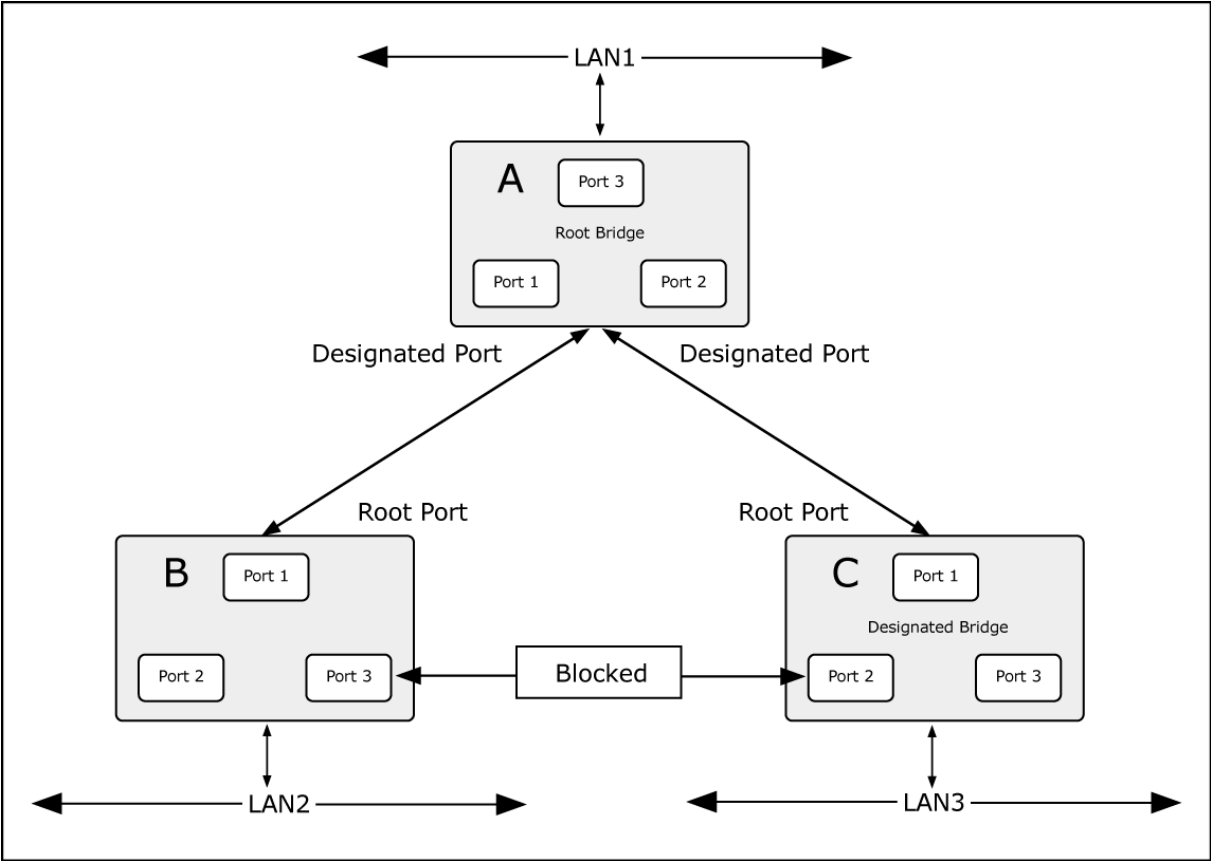


Figure 4-8-3: After Applying the STA Rules

4.8.3 STP Parameters

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.



Note

On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.

On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the switch’s MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC.	32768 + MAC

Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge.	32768
Hello Time	The length of time between broadcasts of the hello message by the switch.	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port.	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path.	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 – Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768



The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.



Observe the following formulas when setting the above parameters:

Max. Age _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

4.8.4 STP System Configuration

This section provides STP-System Configuration from the Managed Switch, the screen in [Figure 4-8-4](#) appears.

- The user can view spanning tree information of Root Bridge.
- The user can modify STP state. After modification, click **Apply**.

Spanning Tree

System Configuration**PerPort Configuration**

Configure Spanning Tree Parameters

STP State (Default DISABLE)	☒
STP protocol version (Default MSTP)	MSTP
Priority (0-61440; Default 32768)	32768
Maximum Age (6-40; Default 20)	20
Hello Time (1-10; Default 2)	2
Forward Delay (4-30; Default 15)	15

Apply**Help**

Figure 4-8-4: STP System Configuration interface

The page includes the following fields:

Object	Description
STP State:	The user must enable the STP function first before configuring the related parameters.
Protocol Version	A value used to specify the spanning tree protocol, the original spanning tree protocol (STP, 802.1D) or the multiple spanning tree protocol (MSTP, 802.1s).
Priority (0-61440):	The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.

Max Age (6-40):	The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
Hello Time (1-10):	The time that controls the switch to send out the BPDU packet to check STP current status. Enter a value between 1 through 10.
Forward Delay Time (4-30):	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.



Note

Follow the rule as below to configure the MAX Age, Hello Time, and Forward Delay Time.
 $2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$.



Note

Each switch in a spanning-tree adopts the Hello Time, Forward Delay time, and Max Age parameters of the root bridge, regardless of how it is configured.

■ Root Bridge Information

This page provides a status overview for all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

The STP Bridge Status screen in [Figure 4-8-5](#) appears.

Root Bridge Information	
Priority	32768
MAC Address	00:00:4F:26:20:D1
Root Path Cost	0
Root Port	PORT140
Maximum Age	20
Hello Time	2
Forward Delay	15

Figure 4-8-5: STP Bridge Status page screenshot

The page includes the following fields:

Object	Description
Priority	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
MAC Address	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Root Port	The switch port currently assigned the <i>root</i> port role.
Maximum Age	Path Cost to the Designated Root for the Root Bridge.
Hello Time	Minimum time between transmissions of Configuration BPDUs.
Forward Delay	Derived value of the Root Port Bridge Forward Delay parameter.

4.8.5 Port Configuration

This web page provides the port configuration interface for STP. You can assign higher or lower priority to each port. Spanning tree protocol will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

Spanning Tree

System Configuration

PerPort Configuration

Configure Spanning Tree Port Parameters

Port Number	Path Cost (1-200000000)	Priority (0 - 240; Default 128)	Admin Edge (Default NO)	Admin Non-STP (Default NO)	Admin P2P (Default AUTO)
Port1 Port2 Port3 Port4 Port5	200000	128	NO	NO	AUTO

Apply

Help

STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P
Port1	2000000	128	Disabled	NO	NO	NO
Port2	2000000	128	Disabled	NO	NO	NO
Port3	200000	128	Forwarding	NO	NO	YES
Port4	2000000	128	Disabled	NO	NO	NO
Port5	2000000	128	Disabled	NO	NO	NO
Port6	2000000	128	Disabled	NO	NO	NO

Figure 4-8-6: STP Port Configuration interface

The page includes the following fields:

Object	Description
Path Cost:	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
Priority:	Decide which port should be blocked by setting its priority as the lowest. Enter a number between 0 and 240. The value of priority must be the multiple of 16.

Admin P2P:

The rapid state transitions possible within STP are dependent upon whether the port concerned can only be connected to exactly another bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively.

- **YES** means the port is regarded as a point-to-point link.
- **NO** means the port is regarded as a shared link.
- **AUTO** means the link type is determined by the auto-negotiation between the two peers.

Admin Edge:

The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "**YES**" status.

Admin Non STP:

The port includes the STP mathematic calculation.

- **YES** is not including STP mathematic calculation.
- **NO** is including the STP mathematic calculation.



Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 4-8-1: Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 4-8-2: Recommended STP Path Costs

4.9 DHCP Relay & Option 82

The Relay Agent Information option (**Option82**) is inserted by the **DHCP relay** agent when forwarding client-originated DHCP packets to a DHCP server (RFC 3046). Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies.

The DHCP Relay can forward the DHCP broadcast packets to a DHCP server in a different subnet (RFC 1542). So DHCP server can provide IP addresses to clients spanning multiple subnets instead of deploying a DHCP server on every subnet.

Configuring DHCP Relay & Option82

To configure DHCP Option82

1. Enable global option82 function: select DHCP Option82 enable "Enable".
2. Enable port option82 function: select Option82 checkbox for special port.
3. Select DHCP Router Port.
4. Click Apply.

To configure DHCP Relay

5. Enable global Relay function: select DHCP Relay enable "Enable".
6. Enable port Relay function: Type the IP addresses of the DHCP "Relay IP".
7. DHCP Server offers an IP address to client from its list of scopes, which subnet is same as the Relay IP.
8. Select DHCP Router Port.
9. Click Apply.

DHCP Relay & Option 82

DHCP Option 82 Disable ▾

DHCP Relay Disable ▾

DHCP Option 82 Router Port Port1 ▾

DHCP Opt.82 Port	Option	Relay IP
Port1	☐	0.0.0.0
Port2	☐	0.0.0.0
Port3	☐	0.0.0.0
Port4	☐	0.0.0.0
Port5	☐	0.0.0.0
Port6	☐	0.0.0.0
Port7	☐	0.0.0.0
Port8	☐	0.0.0.0
Port9	☐	0.0.0.0
Port10	☐	0.0.0.0

Apply
Default
Help

Figure 4-9-1: DHCP Relay & Option 82

The page includes the following fields:

Object	Description
DHCP Option 82	Enable global option82 function
DHCP Relay	Enable global Relay function
DHCP Option 82 Router Port	Select the Router Port that is used to connect to the DHCP server in the domain
DCHP Opt.82 Port	Identify Port-1 to Port-10 to configure DHCP option 82
Option	Enable port option82 function on selected port.
Relay IP	Type the IP addresses of the DHCP "Relay IP".

4.10 LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in **Type Length Value (TLV)** format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

4.10.1 LLDP Configuration

Use this page to change LLDP parameters.

Figure 4-10-1: LLDP Configuration

The page includes the following fields:

Object	Description
LLDP Status	Enable/Disable LLDP.
LLDP hello time	You can change LLDP hello time value. The time interval between the transmission LLDP info packets. Value range is from 5 to 32768. Default value is 30.
LLDP hold time	You can change LLDP hold time value. (The hold time * the hello time) is the TTL time in the LLDP info packets. Value range is from 2 to 10. Default value is 4.

4.10.2 PerPort Configuration

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Configuration screen in [Figure 4-10-2](#) appears.

LLDP Configuration

LLDP Configuration
PerPort Configuration

Configure Port Status

Port Number	Port Status
Port1 ▲ Port2 ☰ Port3 ▼ Port4 ▼ Port5 ▼	Tx_only ▼

Apply
Help

Port Status

PortNum	Status
Port1	Tx_and_Rx
Port2	Tx_and_Rx
Port3	Tx_and_Rx
Port4	Tx_and_Rx

Figure 4-10-2: LLDP per port Configuration

The page includes the following fields:

Object	Description
LLDP Status	Enable/Disable LLDP.
LLDP hello time	You can change LLDP hello time value. The time interval between the transmission LLDP info packets. Value range is from 5 to 32768. Default value is 30.
LLDP hold time	You can change LLDP hold time value. (The hold time * the hello time) is the TTL time in the LLDP info packets. Value range is from 2 to 10. Default value is 4.
Port Status	You can change LLDP port status to Tx_only/Rx_only/Tx_and_Rx/Disable. Tx_only: LLDP transmit the packet of the port only. Rx_only: LLDP receive the packet of the port only. Tx_and_Rx: LLDP transmit and receive the packets of the port. Disable: LLDP do not transmit and receive the packets of the port.

4.11 Access Control List

The **Access Control List (ACL)** is a concept in computer security used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request, principally the process's user identifier. **Access Control List (ACL)** is a mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted or denied to access the resource. The screen in following screen appears.

Packets can be forwarded or dropped by ACL rules include IPv4 or non-IPv4. The Managed Switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

※Packet Type / Binding§ can be selected to ACL for IPv4 or Non-IPv4.

Access Control List

Group Id	(1~220)				
Action	Permit ☐ QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage)				
VLAN	☒ Any ☐ VID 1 (1~4094; Any means Vid=0 if uses binding)				
Packet Type / Binding	☒ IPv4		☐ Non-IPv4		☐ Binding
Src IP Address	☒ Any ☐ IP 0.0.0.0 Mask 255.255.255.255	Ether Type	Any Type#	MAC Address	00:11:22:33:44:55
Dst IP Address	☒ Any ☐ IP 0.0.0.0 Mask 255.255.255.255			IP Address	0.0.0.0
IP Fragment	Uncheck			Port Id	1 (1~10)
L4 Protocol	☒ Any Protocol#	QoS VoIP	Priority#	7	
	☐ TCP Any		PortID#	Value (Hex,0~1F)	Mask (Hex,0~1F)
	☐ UDP Any		Protocol#	Value (Hex,0~FF)	Mask (Hex,0~FF)
	Port#		Source Port#	Value (Hex,0~FFFF)	Mask (Hex,0~FFFF)
			Destination Port#	Value (Hex,0~FFFF)	Mask (Hex,0~FFFF)
Port Id	0 (1~10 ,0:don't care)				
Current List					

Figure 4-11-1: Access Control List (ACL) Web Page screen

The page includes the following fields:

■ IPv4 ACL

Object	Description	Default Value
Group ID	1 ~ 220 (max. 220 ACL group).	
Action	Permit / Deny. ■ Permit: Permit packet cross switch. ■ Deny: Drop packet.	Permit
VLAN	Any / VID. ■ Any: Any VLAN ID. ■ VID: 1~4094. A certain VLAN ID.	Any
Packet Type	IPv4 / Non-IPv4 / Binding ■ IPv4: Set IPv4 packet field. ■ Non-IPv4: Set non-IPv4 packet field. ■ Binding: Set binding entry.	IPv4
Src IP Address	Set this field if Packet Type is IPv4, else ignore. Any / IP and Mask ■ Any: Any IP address. ■ IP: A certain IP address. Mask: *.*.*.*.*.*.* * is represent a digit from 0~9, *** is range from 0 to 255 Notice: This is not subnet mask.	Any
Dst IP Address	Set this field if Packet Type is IPv4, else ignore. Any / IP and Mask ■ Any: Any IP address. ■ IP: A certain IP address. Mask: *.*.*.*.*.*.* * is represent a digit from 0~9, *** is range from 0 to 255	Any
IP Fragment	Set this field if Packet Type is IPv4, else ignore. Uncheck / Check ■ Uncheck: Not check IP fragment field. ■ Check: Check IP fragment field.	Uncheck
L4 Protocol	Set this field if Packet Type is IPv4, else ignore. Any / ICMP(1) / IGMP(2) / TCP(6) / UDP(17)	Any
Protocol	Set this field if Packet Type is IPv4, else ignore. 0~255. If protocol not find in L4 Protocol field, you can direct assign number.	

TCP	Set this field if Packet Type is IPv4, else ignore. Any / FTP(21) / HTTP(80)	Any
Port	Set this field if Packet Type is IPv4, else ignore. 0~65535 If TCP port not find in TCP field, you can direct assign number.	
UDP	Set this field if Packet Type is IPv4, else ignore. Any / DHCP(67) / TFTP(69) / NetBIOS(137)	Any
Port	Set this field if Packet Type is IPv4, else ignore. 0~65535 If UDP port not find in UDP field, you can direct assign number.	
Port ID	Source port ID, from 1~10, 0 means don't care.	0
Current List	You create ACL and Binding groups.	

■ Non-IPv4 ACL

In ※Packet Type / Binding box should select ※Non-IPv4

Object	Description	Default Vaule
Group ID	1 ~ 220 (max. 220ACL group)	
Action	Permit / Deny. ■ Permit: Permit packet cross switch. ■ Deny: Drop packet.	Permit
VLAN	Any / VID. ■ Any: Any VLAN ID. ■ VID: 1~4094. A certain VLAN ID.	Any
Packet Type	IPv4 / Non-IPv4 / Binding ■ IPv4: Set IPv4 packet field. ■ Non-IPv4: Set non-IPv4 packet field. ■ Binding: Set binding entry.	IPv4
Ether Type	Set this field if Packet Type is Non-IPv4, else ignore.) Any / ARP(0x0806) / IPX(0x8137)	Any
Type	Set this field if Packet Type is Non-IPv4, else ignore.) 0~0xFFFF If ether type not find in Ether Type field, you can direct assign number.	
Current List	You create ACL and Binding groups.	

■ Binding

Let device that has specific IP address and MAC address can use network. We can set specific IP address, MAC address, VLAN ID and port ID to bind, and device can cross switch if all conditions match.

Use binding function; we should enable it first in following page.

In ※Packet Type / Binding box should select ※Binding.

Object	Description	Default Value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. ■ Permit: Permit packet cross switch. ■ Deny: Drop packet.	Permit
VLAN	Any / VID. ■ Any: Any VLAN ID. ■ VID: 1~4094. A certain VLAN ID.	Any
Packet Type	IPv4 / Non-IPv4 / Binding ■ IPv4: Set IPv4 packet field. ■ Non-IPv4: Set non-IPv4 packet field. ■ Binding: Set binding entry.	IPv4
MAC Address	**.***.***.***.*** * is represent a digit from 0~9 and A~F, *** is range from 0 to FF.	00:11:22:33:44:55
IP Address	***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255.	0.0.0.0
Port ID	Source port ID, from 1~10. 0 means don't care.	1
Current List	You create ACL and Binding groups.	

4.12 Security Manager

This section provides the User Name and the Password assign or the Password Change of VDSL Managed Switch, the screen in [Figure 4-12-1](#) appears the User Name and the Password Setting object of VDSL Managed Switch.



The Security Manager web page features a title 'Security Manager' at the top. Below it, there are three input fields: 'User Name', 'Assign/Change password', and 'Reconfirm password'. Each field is preceded by a label in a grey box. At the bottom center, there is an 'Apply' button.

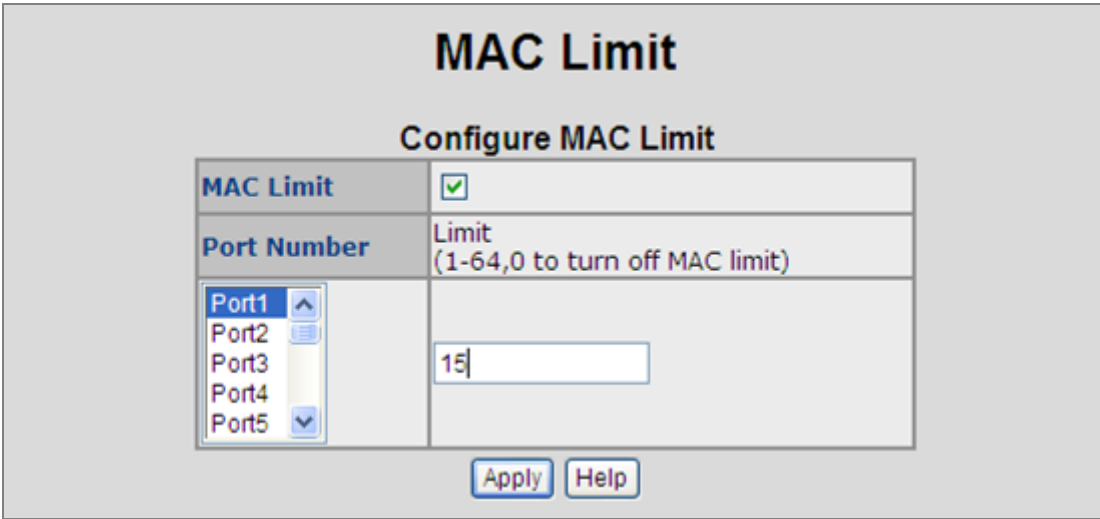
Figure 4-12-1: Security Manager Web Page screen

4.13 MAC Limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

4.13.1 MAC Limit Configuration

The Layer 2 MAC Limit function can be per-port configured for security management purposes. When the port is in MAC Limit mode, the port will be "locked" without permission of address learning. Only the incoming packets with Source MAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses.



The MAC Limit configuration screen has a title 'MAC Limit' and a subtitle 'Configure MAC Limit'. It contains a table with two columns. The first column has labels 'MAC Limit' and 'Port Number'. The second column has a checkbox for 'MAC Limit' (checked), a text input for 'Limit' (1-64, 0 to turn off MAC limit), and a dropdown menu for 'Port Number' (showing Port1, Port2, Port3, Port4, Port5). Below the table, there are 'Apply' and 'Help' buttons.

Figure 4-13-1: MAC Limit - Configure MAC Limit

The page includes the following fields:

Object	Description
MAC Limit	Enable or disable MAC limit function for the Managed Switch.
Port Number	Indicate port 1 to port 8.
Limit	The maximum number of per-port MAC addresses to be learned (1-64, 0 to disable this port's MAC limit function).



MAC Limit is only functioned on Fast Ethernet port, the Port-1 to Port-8 of VCO-8 (or Port-1 to Port-24 of VCO-24).

4.13.2 MAC Limit Port Status

This table displays current MAC Limit status of each port.

MAC Limit Port Status	
Port Number	Limit
Port1	off
Port2	off
Port3	off
Port4	off
Port5	off
Port6	off
Port7	off
Port8	off

Figure 4-13-2: MAC Limit – MAC Limit Port Status

The page includes the following fields:

Object	Description
Port Number	Indicate port 1 to port 8.
Limit	Display the current MAC Limit configuration and status of each port.

4.14 802.1x Configuration

802.1x is an IEEE authentication specification which prevents the client from accessing a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

4.14.1 Understanding IEEE 802.1x Port-Based Authentication

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1x access control allows only **Extensible Authentication Protocol over LAN (EAPOL)** traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ Device Roles

With 802.1x port-based authentication, the devices in the network have specific roles as shown below.

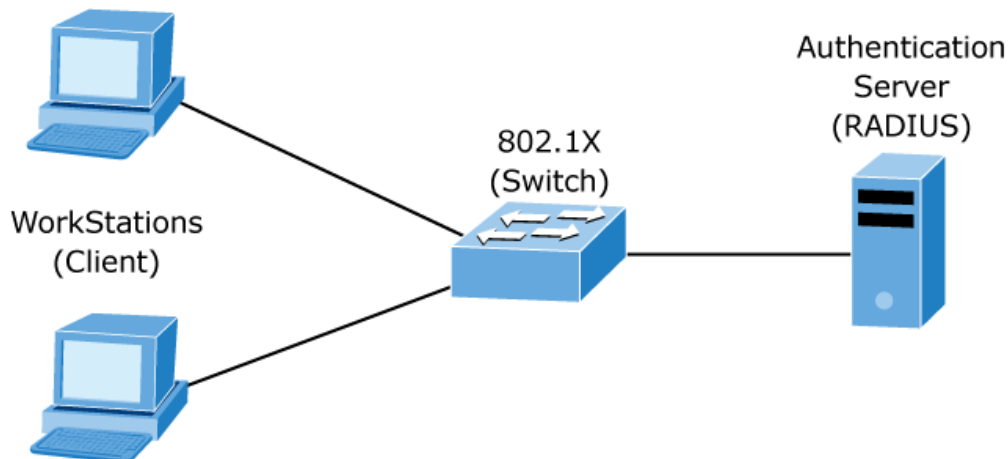


Figure 4-14-1: 802.1x device role

Client—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the supplicant in the IEEE 802.1x specification.)

- **Authentication server**—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible Authentication**

Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- **Switch (802.1x device)**—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.



If 802.1x is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. “[Figure 4-14-2](#)” shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

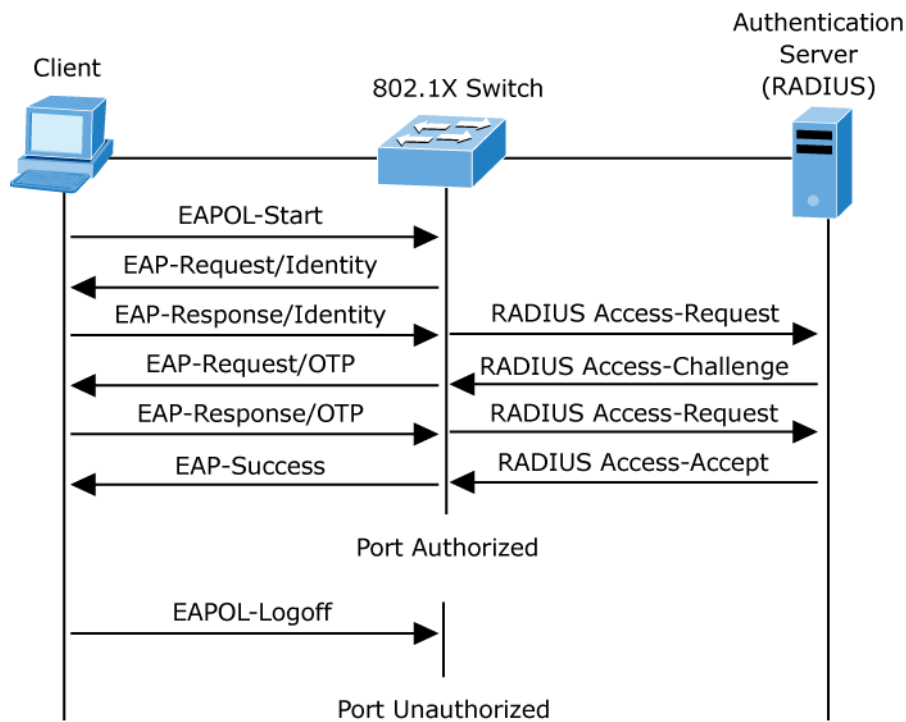


Figure 4-14-2: EAP message exchange

■ Ports in Authorized and Unauthorized States

The switch port state determines whether or not the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1x protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1x is connected to an unauthorized 802.1x port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1x-enabled client connects to a port that is not running the 802.1x protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

4.14.2 System Configuration

802.1x makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

To enable 802.1x, from **System \ System Information \ Misc Config** then you still to fill in the authentication server information :

The screenshot shows a configuration window for the 802.1x Protocol. It includes several options and settings:

- Broadcast Storm Filter Packet select:**
 - ☐ Broadcast Packets
 - ☐ IP Multicast
 - ☐ Control Packets
 - ☐ Flooded Unicast/Multicast Packets
- Collisions Retry Forever :** 16 (dropdown)
- Hash Algorithm :** CRC-Hash (dropdown)
- IP/MAC Binding :** Disable (dropdown)
- 802.1x Protocol :** Enable (dropdown)

At the bottom, there are three buttons: **Apply**, **Default**, and **Help**.

Figure 4-14-3: System information \ Misc Configuration\ 802.1x Protocol

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

The screenshot shows the **802.1x Configuration** interface. It has three tabs: **System Configuration** (selected), **PerPort Configuration**, and **Misc Configuration**. Under the **System Configuration** tab, there is a section titled **Configure 802.1x Parameters** with the following fields:

Radius Server IP:	192.168.0.99
Server Port:	1812
Accounting Port:	1813
Shared Key:	
NAS,Identifier:	NAS_L2_SWITCH

At the bottom, there are two buttons: **Apply** and **Help**.

Figure 4-14-4: 802.1x System Configuration interface

The page includes the following fields:

Object	Description
Radius Server IP:	Assign the RADIUS Server IP address.
Server Port:	Set the UDP destination port for authentication requests to the specified RADIUS Server.
Accounting Port:	Set the UDP destination port for accounting requests to the specified RADIUS Server.
Shared Key:	Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
NAS, Identifier:	Set the identifier for the RADIUS client.

4.14.3 802.1x PerPort Configuration

In this page, you can select the specific port and configure the authorization state. The state provides **No Authorization**, **Force Authorized**, **Force unauthorized**, and **Authorize**.

802.1X Configuration

System Configuration **PerPort Configuration** Misc Configuration

Configure 802.1X Per Port State

Port Number	Port State
Port1	Au ▼
Port2	
Port3	
Port4	
Port5	

Apply Help

Port Status

PortNum	State
Port1	No
Port2	No
Port3	No
Port4	No

Figure 4-14-5: 802.1x PerPort Setting interface

The page includes the following fields:

Object	Description
Fu (Force Unauthorized)	The specified port is required to be held in the unauthorized state.
Fa (Force Authorized)	The specified port is required to be held in the authorized state.
Au (Authorize)	The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
No	The specified port works without complying with 802.1x protocol.

4.14.4 Misc Configuration

In this page, you can change the default configuration for the 802.1x standard:

802.1x Configuration

System Configuration
PerPort Configuration
Misc Configuration

Configure 802.1x misc configuration

Quiet period:	60
Tx period:	15
Supplicant timeout:	30
Server timeout:	30
Max requests:	2
Reauth period:	3600

Figure 4-14-6: 802.1x Misc Configuration interface

The page includes the following fields:

Object	Description
Quiet Period:	Used to define periods of time during which it will not attempt to acquire a supplicant. Default time is 60 seconds.
TX Period:	Set the period the port waits for retransmit next EAPOL PDU during an authentication session. Default value is 30 seconds.
Supplicant Timeout:	Set the period of time the switch waits for a supplicant response to an EAP request. Default value is 30 seconds.
Server Timeout:	Set the period of time the switch waits for a server response to an authentication request. Default value is 30 seconds.
Max Requests:	Set the number of authentication that must time-out before authentication fails and the authentication session ends. Default value is 2 times.
Reauth period:	Set the period of time which clients connected must be re-authenticated. Default value is 3600 seconds.

4.15 QoS Configuration

4.15.1 Understand QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

The **QoS** page of the Switch contains three types of QoS mode - the **CoS** mode, **TOS** mode or **Port-based** mode can be selected. Both the three mode rely on predefined fields within the packet to determine the output queue.

- **CoS / 802.1p Tag Priority Mode** –The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- **TOS / DSCP Mode** - The output queue assignment is determined by the TOS or DSCP field in the IP packets.
- **Port-Based Priority Mode** – Any packet received from the specify high priority port will treated as a high priority packet.

4.15.2 QoS Configuration

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. When CoS / 802.1p Tag Priority is applied, the Switch recognizes 802.1Q VLAN tag packets and extracts the VLAN tagged packets with User Priority value.

802.1Q Tag and 802.1p priority

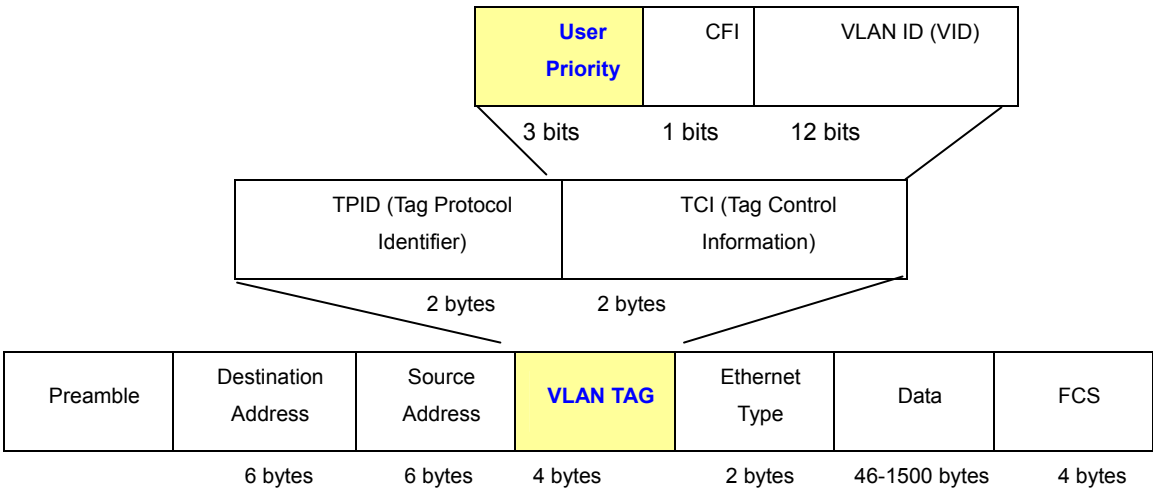


Figure 4-15-1: 802.1p Tag Priority

Set up the COS priority level. With the drop-down selection item of Priority Type above being selected as COS only/COS first, this control item will then be available to set the queuing policy for each port.

4.15.2.1 Priority Queue Service settings

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. The IEEE 802.1p Priority specification uses 8 priority levels to classify data packets. In 802.1p compliant devices, a tag inserted into the packet header is used to identify the priority level of data packets.

The Switch supports Static Port Ingress priority and four queues. The screen in [Figure 4-15-2](#) appears.

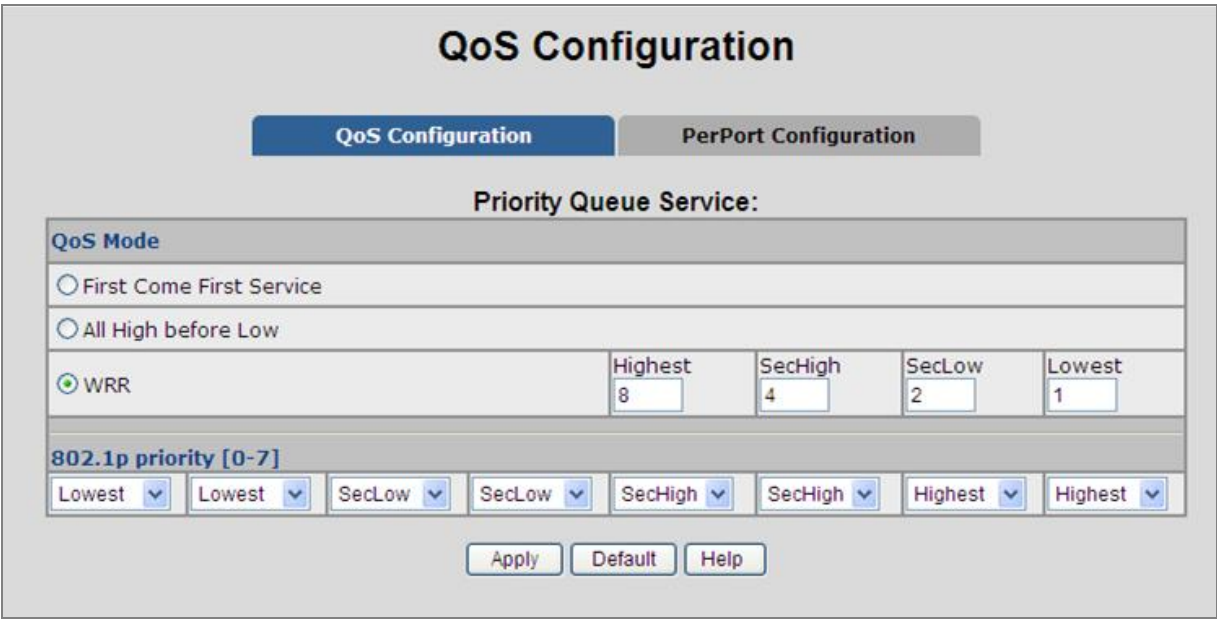


Figure 4-15-2: QoS Configuration – 802.1Priority

The table includes the following fields:

Object	Description
First Come First Service	The sequence of packets sent depends on arrival order.
All High before Low	The high priority packets sent before low priority packets.
	Select the preference given to packets in the switch's higher-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent.
Weighted Round Robin	For example, 8 Highest : 4 SecHigh : 2 SecLow : 1 Lowest means that the switch sends 8 highest priority packets before sending 4 second high priority packet, before sending 2 second low priority packet, before sending 1 lowest priority packet.
802.1p priority [0-7]	Set up the COS priority level 0~7— High, Middle, Low, Lowest .



Note

802.1p Priority: Priority classifiers of the Switch forward packet. COS range is from 0 to 7. Seven is the high class. Zero is the less class. The user may configure the mapping between COS and Traffic classifiers.

4.15.2.2 QoS PerPort Configuration

Configure the priority level for each port. With the drop-down selection item of Priority Type above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

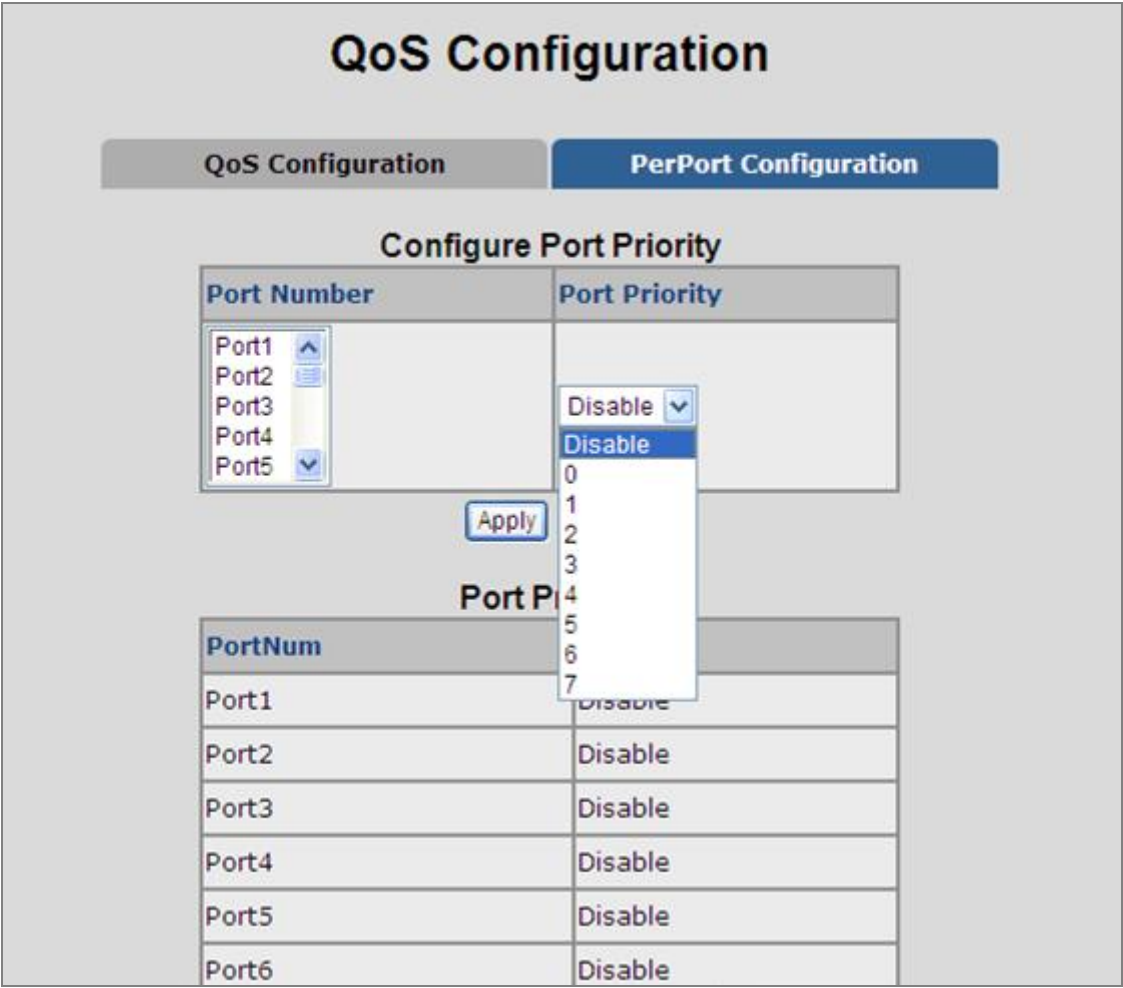


Figure 4-15-3: QoS Configuration – Port-Based Priority

The table includes the following fields:

Object	Description
Port Number:	Indicate port 1 to port 10.
Port Priority:	Each port has 8 priority levels—0~7 or Disable to be chosen. 7 is the highest priority.

4.15.3 TOS/DSCP

TOS/DSCP priority is obtained through a 6-bit **Type-of-Service (TOS)** or **Differentiated Service Code Point (DSCP)** to 3-bit priority mapping.

The **Type of Service (TOS)** octet in the IPv4 header is divided into three parts; Precedence (3 bits), TOS (4 bits), and MBZ (1 bit). The Precedence bits indicate the importance of a packet, whereas the TOS bits indicate how the network should make tradeoffs between throughput, delay, reliability, and cost (as defined in RFC 1394). The MBZ bit (for “must be zero”) is currently unused and is either set to zero or just ignored.

0	1	2	3	4	5	6	7
Precedence			TOS				MBZ

IPv4 Packet Header Type of Service Octet

The four TOS bits provide 15 different priority values, however only five values have a defined meaning.

DiffServ Code Point (DSCP) — is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network. DSCP are defined in RFC2597 for classifying traffic into different service classes. The Managed Switch extracts the codepoint value of the DS field from IPv4 packets and identifies the priority of the incoming IP packets based on the configured priority.

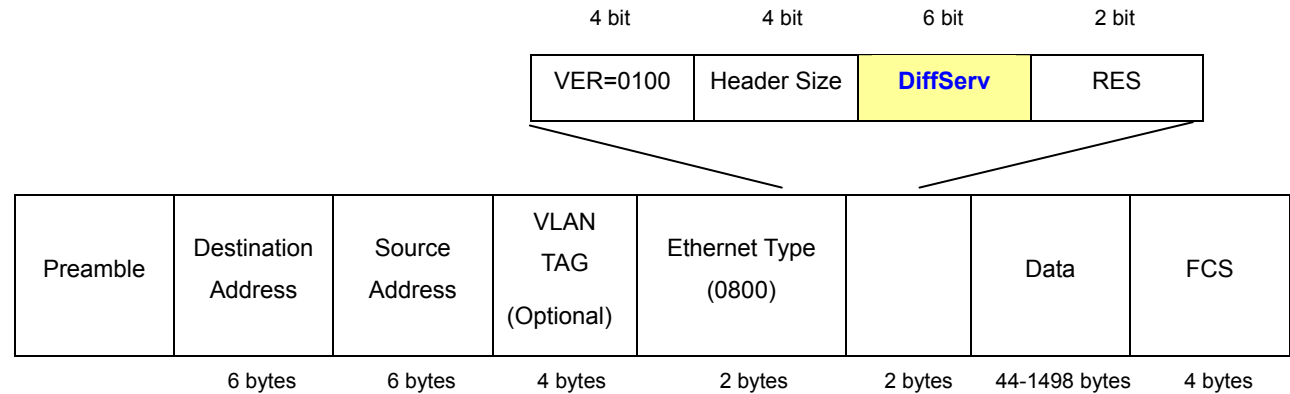


Figure 4-15-4: IPv4 frame format

The DSCP is **six bits** wide, allowing coding for up to 64 different forwarding behaviors. The DSCP retains backward compatibility with the three precedence bits so that non-DSCP compliant, TOS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

4.15.3.1 TOS/DSCP Configuration

The **TOS/DSCP** page provides fields for defining output queue to specific DSCP fields. When TCP/IP's TOS/DSCP mode is applied, the Managed Switch recognizes TCP/IP Differentiated Service Codepoint (DSCP) priority information from the DS-field defined in RFC2474.

Enable TOS/DSCP for traffic classification and then the DSCP to priority mapping column is configurable, as the [Figure 4-15-5](#) shows:

DSCP	Priority
DSCP1	0
DSCP2	0
DSCP3	0
DSCP4	0
DSCP5	0
DSCP6	0
DSCP7	0
DSCP8	0
DSCP9	0
DSCP10	0

Figure 4-15-5: QoS Configuration – TOS Priority

The page includes the following fields:

Object	Description
TOS/DSCP	Enable / Disable internal traffic class (0~7) to map the corresponding IP DSCP value.
DSCP	The values of the IP DSCP header field within the incoming packet. 0~63.
Priority	Specify which 802.1p priority to map the corresponding IP DSCP. The value is 0~7.

4.15.3.2 TOS/DSCP Port Configuration

Set up IP TOS / DSCP mapping to 802.1p priority when receiving IPv4 packets, the Managed Switch allow to by port configuring the QoS Status. This TOS/DSCP Port Configuration page is to configure the IP TOS/DSCP mapping on the port and display the current port status. The screen in [Figure 4-15-6](#) appears.

TOS/DSCP

TOS/DSCP Configuration

TOS/DSCP Port Configuration

Configure Port TOS/DSCP Status

Port Number	TOS/DSCP Status
Port1	Disable
Port2	
Port3	
Port4	
Port5	

Apply Help

TOS/DSCP Port Status

PortNum	TOS/DSCP Port Status
Port1	Enable
Port2	Enable
Port3	Enable
Port4	Enable
Port5	Disable
Port6	Disable

Figure 4-15-6: QoS Configuration – TOS/DSCP Port Status

The table includes the following fields:

Object	Description
Port Number	Indicate port 1 to port 10.
TOS/DSCP Status	Enable / Disable TOS/DSCP map to 802.1p priority on specify port.

4.16 VDSL Configuration

VDSL2 (Very High-Bit-Rate Digital Subscriber Line 2), G.993.2 is the newest and most advanced standard of xDSL broadband wire line communications. Designed to support the wide deployment of Triple Play services such as voice, data, high definition television (HDTV) and interactive gaming, VDSL2 enable operators and carrier to gradually, flexibly, and cost efficiently upgrade exiting xDSL-infrastructure.

VDSL2 was developed and standardized in record time to address the shortcomings of existing access technologies. It servers as the ideal xDSL technology for eliminating last-mile bottlenecks and enable global mass deployment of advance Triple Play services. Unlike its predecessor, which allowed choosing either **DMT (Discrete Multi-Tone)** or QAM (Quadrature Amplitude Modulation) technology, VDSL2 only uses the DMT line code.

DMT is a method of separating a DSL signal so that the usable frequency range is separated into multiple small frequency bands, or tone. It uses up to 4096 tones which are spaced 4 kHz or 8 kHz apart. Each tone can be used for either downstream or upstream.

The VDSL2 Managed Switch can provide very high performance access to remote CPE, both downstream and upstream up to 100Mbps. The VDSL2 Managed Switch complies with ITU-T G993.2 standard, and supports CO operating mode. The CO by WEB UI and users can connect to multiple CPE for Point-to-Multi-Point Application, data transmission between multiple networks over existing copper telephone lines.

4.16.1 Profile Configuration

This option allows you to setup the VDSL configuration profile. From the **VDSL Configuration** menu, please click on VDSL Configuration Profile. The following page is displayed.

Profile Setting

Status : Load OK

Configuration

Profile Table

User profile name

default

New profile Name

(Max 64 bytes)

system profile name

AnnexA_R_POTS_D-32_EU-32_12b

SNR

Ds: 6dB

Us: 6dB

Rate limit Ds Us

Ds: 101 Mb/s

Us: 101 Mb/s

INP 30a

Ds: 2 symbol

Us: 2 symbol

INP no 30a

Ds: 2 symbol

Us: 2 symbol

MaxDelay

Ds: 8ms

Us: 8ms

Port

Add

<< Remove

Port1

Port2

Port3

Port4

Port5

Port6

Port7

Port8

New

Set

Delete

Figure 4-16-1: VDSL2 Profile Configuration interface

The page includes the following fields:

Object	Description
User Profile Name	This field shows the index name of the profile. Click on the drop-down list and select the index profile name to be created or configured.
New Profile Name	Type in profile name when you're creating a new profile. The allowed characters include: 0-9, A-Z, a-z, "_" and "-". Maximum 64 bytes.
System Profile Name	The VDSL2 Managed Switch provides most common VDSL2 profiles for user; it supports the 30a, 17a, 12a, 12b, 8a, 8b, 8c and 8d. You can select the proper profile for your real environment. Different profiles provide different connection status of data rate and distance; please refer to Appendix A for more information. Click on the drop-down list and select the VDSL band plan to be used. The VDSL2 Managed Switch supports below profiles. 1. AnnexA_R_POTS_D-32_EU-32_30a 2. AnnexA_R_POTS_D-32_EU-32_17a 3. AnnexA_R_POTS_D-32_EU-32_12b 4. AnnexA_R_POTS_D-32_EU-32_12a 5. AnnexA_R_POTS_D-32_EU-32_8a 6. AnnexA_R_POTS_D-32_EU-32_8b 7. AnnexA_R_POTS_D-32_EU-32_8c 8. AnnexA_R_POTS_D-32_EU-32_8d 9. AnnexA_R_POTS_D-64_EU-64_30a_NUS0 10. AnnexA_R_POTS_D-64_EU-64_17^a 11. AnnexB_B7-1_997-M1c-A-7 12. AnnexB_B7-2_997-M1x-M-8 13. AnnexB_B7-3_997_M1x-M 14. AnnexB_B7-4_997_M2x-M-8 15. AnnexB_B7-5_997_M2x-A 16. AnnexB_B7-6_997_M2x-M 17. AnnexB_B7-9_997E17-M2x-A 18. AnnexB_B7-10_997E30-M2x-NUS0 19. AnnexB_B8-1_998-M1x-A 20. AnnexB_B8-2_998-M1x-B 21. AnnexB_B8-4_998-M2x-A 22. AnnexB_B8-5_998-M2x-M 23. AnnexB_B8-6_998-M2x-B 24. AnnexB_B8-8_998E17-M2x-NUS0 25. AnnexB_B8-9_998E17-M2x-NUS0-M 26. AnnexB_B8-10_998ADE17-M2x-NUS0-M 27. AnnexB_B8-11_998ADE17-M2x-A 28. AnnexB_B8-12_998ADE17-M2x-B 29. AnnexB_B8-13_998E30-M2x-NUS0 30. AnnexB_B8-14_998E30-M2x-NUS0-M 31. AnnexB_B8-15_998ADE30-M2x-NUS0-M 32. AnnexB_B8-16_998ADE30-M2x-NUS0-A 33. AnnexC_POTS_25-138_b 34. AnnexC_POTS_25-276_b

35. AnnexC_TCM-ISDN

SNR

The line quality is determined by using the **SNR (Signal to Noise Ratio)** and applies to VDSL line connections only. SNR is the ratio of the amplitude of the actual signal to the amplitude of noise signals at a given point in time. The higher the SNR is, the better the line quality. Please manually adapt SNR margin according to line quality and distance to get better performance or replace the line with new one.

Click on the drop-down list and select the SNR to be used. Configures SNR margin of Downstream or Upstream.

SNR margin value: **6 dB to 24 dB**

Default value: **6 dB**

Rate Limit DS US

- **DS:** Configure the transmit rate of Maximum Downstream. The value of downstream traffic limitation in Mbps, from the VDSL2 CO Managed Switch to the CPE. Per port in step of 1 Mbps and 5Mbps.

Default : **101Mbps/s** (bit per second)

The range between 1Mbps to 101Mbps

- **US:** Configure the transmit rate of Maximum Upstream. The value of upstream traffic limitation in Mbps, from the VDSL2 CPE to the CO Managed Switch. Per port in step of 1 Mbps and 5Mbps.

Default : **101Mbps/s** (bit per second)

The range between 1Mbps to 101Mbps

INP 30a**INP no 30a**

Configure INP with specifying Upstream or Downstream to set minimum protection values of port provision. Click on the drop-down list and select the **INP (Impulse Noise Protection)** to be used.

The range between 1 (or 0.5 for no 30a case) to 16 symbol, or **No Protection**

Default value: **2 symbol**

MaxDelay

The VDSL line type can be configured by selecting **maximum Interleave delay** of Downstream or Upstream direction. Basically, there are three types

- **No limit**
- **Fast mode**
- **Interleave**

The interleave process is use to correct data error before modulation digital signal into analog signal. Interleave prevents error by enhanced correction but may slow down transmit rate because packets are gathered.

Interleaved mode provides impulse noises protection for any impulse noise with a duration less than 250 us. By configuring interleave maximum-delay, it can prevent transmission delay caused of waiting data gathered.

To skip Interleave process, select "No delay" to operate with Fast mode.

Fast mode guarantees a minimum end to end latency less than 1 ms.

Click on the drop-down list and select the MaxDelay to be used. Configures interleave-delay with specifying Downstream or Upstream. The unit is msec.

The range between **0ms** to **63ms**

Default value: **8ms**

Port

In the VDSL2 Managed Switch, all VDSL ports are contained on one profile. To change the member ports to other profile, the "**User Profile Name**" has to be selected first.

Add: Applies Profile to specified ports.

Remove: Disables profile in specified ports.



1. The default profile of VDSL port is "**30a**"
2. If the SNR margin is configured too big, the transmit rate will ne slow down, whereas communications is stable.
3. If the "MaxDelay" is configured to "**No Delay**" (Fast mode), error correction will not be down well, whereas transmit rat of date becomes faster.



Option Band:

AnnexA: use 6 to 32 tone in annex A environment in the direction of upstream.

AnnexB: use 32 to 64 tone in annex B environment in the direction of upstream.

4.16.2 VDSL Port Status

Network manager can check the VDSL Line status in this VDSL Port Status web page; it includes Line status, Upstream / Downstream Data Rate, SNR and VDSL2 firmware version.

VDSL Port Status							
Port	Status	Upstream Rate (Unit:Kb/s)	Downstream Rate (Unit:Kb/s)	SNR Margin (US) (Unit:0.1db)	SNR Margin (DS) (Unit:0.1db)	Firmware Version	Detail
Port1	Showtime	100992	100992	78	249	10201	Advance
Port2	Showtime	100992	100992	63	234	10201	Advance
Port3	Idle	0	0	NA	NA	10201	Advance
Port4	Idle	0	0	NA	NA	10201	Advance
Port5	Idle	0	0	NA	NA	10201	Advance
Port6	Idle	0	0	NA	NA	10201	Advance
Port7	Idle	0	0	NA	NA	10201	Advance
Port8	Idle	0	0	NA	NA	10201	Advance

Figure 4-16-2: VDSL2 Port Status interface

By click the **Advance** button, the windows popup and shows detail VDSL upstream / downstream information on specified port.

Up Stream		Down Stream	
Delay	5 ms	Delay	5 ms
INP	20 0.1 symbols	INP	20 0.1 symbols
CRC 15M	0	CRC 15M	0
CRC 1Day	0	CRC 1Day	0
CRC Total	0	CRC Total	0
Error Correction 15M	0	Error Correction 15M	0
Error Correction 1Day	1195	Error Correction 1Day	0
Error Correction Total	9808	Error Correction Total	456
xdsl2ChStatusPrevDataRate	0 Kbps	xdsl2ChStatusPrevDataRate	0 Kbps
xdsl2LineStatusAttainableRate	105448 Kbps	xdsl2LineStatusAttainableRate	168634 Kbps
xdsl2LineStatusElectricalLength	11 0.1 dB	xdsl2LineStatusElectricalLength	11 0.1 dB
xdsl2LineBandStatusSnrMargin	NA (US0) 0.1dB	xdsl2LineBandStatusSnrMargin	-- (--) 0.1dB
xdsl2LineBandStatusSnrMargin	79 (US1) 0.1dB	xdsl2LineBandStatusSnrMargin	248 (DS1) 0.1dB
xdsl2LineBandStatusSnrMargin	79 (US2) 0.1dB	xdsl2LineBandStatusSnrMargin	248 (DS2) 0.1dB
xdsl2LineBandStatusSnrMargin	77 (US3) 0.1dB	xdsl2LineBandStatusSnrMargin	249 (DS3) 0.1dB
xdsl2LineBandStatusSnrMargin	NA (US4) 0.1dB	xdsl2LineBandStatusSnrMargin	NA (DS4) 0.1dB
xdsl2PMLCurr15MTimeElapsed	733 secs	xdsl2PMLCurr15MTimeElapsed	29 secs
xdsl2PMLCurr15MFecs	0	xdsl2PMLCurr15MFecs	0
xdsl2PMLCurr15MEs	0	xdsl2PMLCurr15MEs	0
xdsl2PMLCurr15MSes	0	xdsl2PMLCurr15MSes	0
xdsl2PMLCurr15MLoss	0	xdsl2PMLCurr15MLoss	0
xdsl2PMLCurr15MUas	0	xdsl2PMLCurr15MUas	0
xdsl2PMLCurr1DayTimeElapsed	60133 secs	xdsl2PMLCurr1DayTimeElapsed	60329 secs
xdsl2PMLCurr1DayFecs	7	xdsl2PMLCurr1DayFecs	0
xdsl2PMLCurr1DayEs	0	xdsl2PMLCurr1DayEs	0
xdsl2PMLCurr1DaySes	0	xdsl2PMLCurr1DaySes	0
xdsl2PMLCurr1DayLoss	0	xdsl2PMLCurr1DayLoss	0
xdsl2PMLCurr1DayUas	0	xdsl2PMLCurr1DayUas	0
xdsl2PMLCurrTotalFecs	0	xdsl2PMLCurrTotalFecs	0
xdsl2PMLCurrTotalEs	0	xdsl2PMLCurrTotalEs	0

Figure 4-16-3: VDSL2 Port Status Advance Information

The page includes the following fields:

Object	Description
Delay	Display the current Interleave delay of the selected VDSL line of Downstream or Upstream direction
INP	Shows the configured INP in VDSL line.
CRC 15M	Shows the numbers of CRC errors in previous 15 minutes. It can be use to check times of error at present time from beginning

	of the 15 minutes and time of error of previous 15 minutes.
CRC 1Day	Shows the numbers of CRC errors in previous day. It can be use to check times of error at present time from starting Today, times of error of yesterday.
CRC Total	Shows the collected data of all errors from booting.
Error Correction 15M	Shows the numbers of error correction in previous 15 minutes.
Error Correction 1Day	Shows the numbers of error correction in previous day.
Error Correction Total	Shows the collected data of all error correction from booting.
xdsl2ChStatusPrevDataRate	The previous net data rate that the bearer channel was operating at just before the latest rate change event. This could be a full or short initialization, fast retrain, DRA or power management transitions, excluding transitions between L0 state and L1 or L2 states. The data rate is coded in bit/s.
xdsl2LineStatusAttainableRateUs	Maximum Attainable Data Rate Upstream. The maximum upstream net data rate currently attainable by the VTU-R transmitter and the VTU-C receiver, coded in bit/s.
xdsl2LineStatusElectricalLength	This parameter contains the estimated electrical length expressed in dB at 1 MHz, k10. This is the final electrical length that would have been sent from the VTU-O to VTU-R if the electrical length was not forced by the CO-MIB. The value ranges from 0 to 128 dB in steps of 0.1 dB.
xdsl2LineBandStatusSnrMargin	SNR Margin is the maximum increase in dB of the noise power received at the VTU (VTU-R for a band in the downstream direction and VTU-C for a band in the upstream direction), such that the BER requirements are met for all bearer channels received at the VTU. Values range from -640 to 630 in units of 0.1 dB (Physical values are -64 to 63 dB). A special value of 0x7FFFFFFF (2147483647) indicates the SNR Margin is out of range to be represented. A special value of 0x7FFFFFFE (2147483646) indicates the SNR Margin measurement is currently unavailable
xdsl2PMLCurr15MTimeElapsed	Total elapsed seconds in this interval
xdsl2PMLCurr15MFecs	Count of seconds during this interval that there was at least one FEC correction event for one or more bearer channels in this line. This parameter is inhibited during UAS or SES
xdsl2PMLCurr15MEs	Count of seconds during this interval that there was: VTU-C: CRC-8 >= 1 for one or more bearer channels OR LOS >= 1 OR SEF >=1 OR LPR >= 1 VTU-R: FEBE >= 1 for one or more bearer channels OR

	LOS-FE >=1 OR RDI >=1 OR LPR-FE >=1 . This parameter is inhibited during UAS
xdsI2PMLCurr15MSes	Count of seconds during this interval that there was: VTU-C: (CRC-8 anomalies in one or more of the received bearer channels) >= 18 OR LOS >= 1 OR SEF >= 1 OR LPR >= 1 VTU-R: (FEBE anomalies in one or more of the received bearer channels) >= 18 OR LOS-FE >= 1 OR RDI >= 1 OR LPR-FE >= 1 . This parameter is inhibited during UAS.
xdsI2PMLCurr15MLoss	Count of seconds during this interval that there was LOS (or LOS-FE for VTU-R
xdsI2PMLCurr15MUas	Count of seconds in Unavailability State during this interval. Unavailability begins at the onset of 10 contiguous severely-errored seconds, and ends at the onset of 10 contiguous seconds with no severely-errored seconds
xdsI2PMLCurr1DayTimeElapsed	Total elapsed seconds in this interval
xdsI2PMLCurr1DayFecs	Count of seconds during this interval that there was at least one FEC correction event for one or more bearer channels in this line. This parameter is inhibited during UAS or SES
xdsI2PMLCurr1DayEs	Count of seconds during this interval that there was: VTU-C: CRC-8 >= 1 for one or more bearer channels OR LOS >= 1 OR SEF >= 1 OR LPR >= 1 VTU-R: FEBE >= 1 for one or more bearer channels OR LOS-FE >= 1 OR RDI >= 1 OR LPR-FE >= 1. This parameter is inhibited during UAS.
xdsI2PMLCurr1DaySes	Count of seconds during this interval that there was: VTU-C: (CRC-8 anomalies in one or more of the received bearer channels) >= 18 OR LOS >= 1 OR SEF >= 1 OR LPR >= 1 VTU-R: (FEBE anomalies in one or more of the received bearer channels) >= 18 OR LOS-FE >= 1 OR RDI >= 1 OR LPR-FE >= 1 . This parameter is inhibited during UAS
xdsI2PMLCurr1DayLoss	Count of seconds during this interval that there was LOS (or LOS-FE for VTU-R
xdsI2PMLCurr1DayUas	Count of seconds in Unavailability State during this interval. Unavailability begins at the onset of 10 contiguous severely-errored seconds, and ends at the onset of 10 contiguous seconds with no severely-errored seconds

5. CONSOLE MANAGEMENT

The VDSL2 Managed Switch series is equipped with a RS-232 DB9 connector as default. And both of the two models support telnet management.

5.1 Login in the Console Interface

To configure the system via console mode, connect a serial cable to a COM port on a PC or notebook computer and to RJ-45 type serial (console) port of the Managed Switch. The console port of the Managed Switch is DCE already, so that you can connect the console port directly through PC without the need of Null Modem.

Please refer to [chapter 3.5- Administration Console](#) to get more information about how to connect to the console interface of VCO-8 with HyperTerminal on Microsoft Windows platform.

Once the terminal has connected to the device, power on the VCO-8, the terminal will display that it is running testing procedures.

Then, the following message asks the login password. The factory default password as following and the login screen in [Figure 5-1-1](#) appears.

```
Username: admin
Password: admin
```

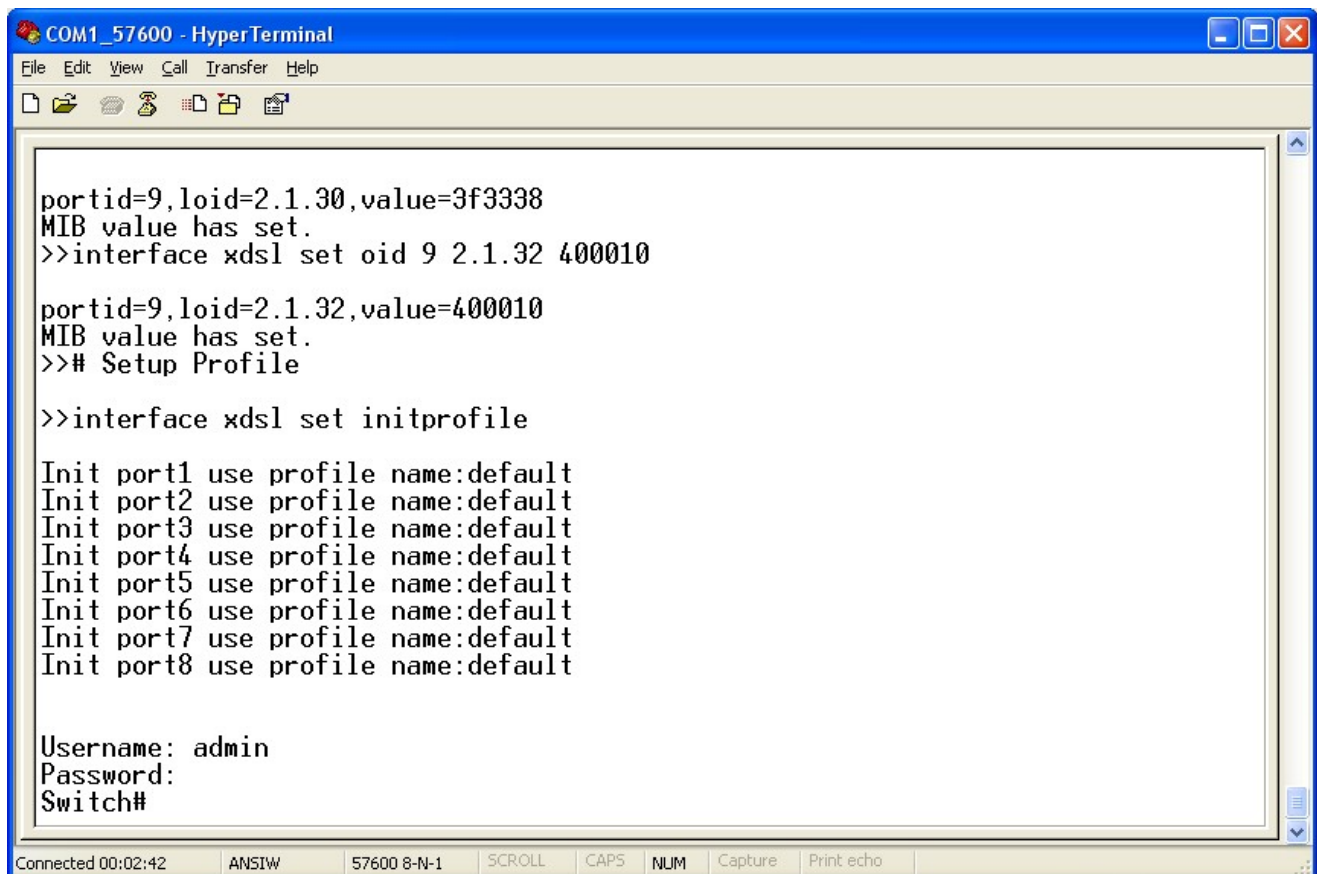


Figure 5-1-1: VDSL2 Managed Switch Console Login screen



1. For security reason, please change and memorize the new username and password after this first setup.
Username Max: **6**, Min: **1** character.
Password Max: **6**, Min: **1** character.
2. Only accept command in lowercase letter under console interface.

5.2 Configure IP address

The VCO-8 Managed Switch is shipped with default IP address as following.

IP Address : **192.168.0.100**
Subnet Mask : **255.255.255.0**

To check the current IP address or modify a new IP address for the Switch, please use the procedures as follow:

■ Show the current IP address

1. On "**Switch#**" prompt, enter "**configure**".
2. On "**Switch(config)#**" prompt, enter "**show ip**".
3. The screen displays the current IP address, Subnet Mask and Gateway. As show in [Figure 5-2-1](#).

```

COM1_57600 - HyperTerminal
File Edit View Call Transfer Help
QinQ.....OK
Forwarding.....OK
IP Mcst.....OK
IGMP.....OK
STP/RSTP/MSTP...OK
MIB.....OK
802.1X.....OK
Port.....OK
ACL.....OK
SNMP.....OK
Port interval...OK
TOS/DSCP.....OK
MAC.....OK
Completed!!

Username: admin
Password:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# _
Connected 00:07:05  ANSIW  57600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo

```

Figure 5-2-1: Show IP information screen

■ Configure IP address

1. On "**Switch(config)#**" prompt, enter the following command and press **<Enter>**. As show in [Figure 5-2-2](#).

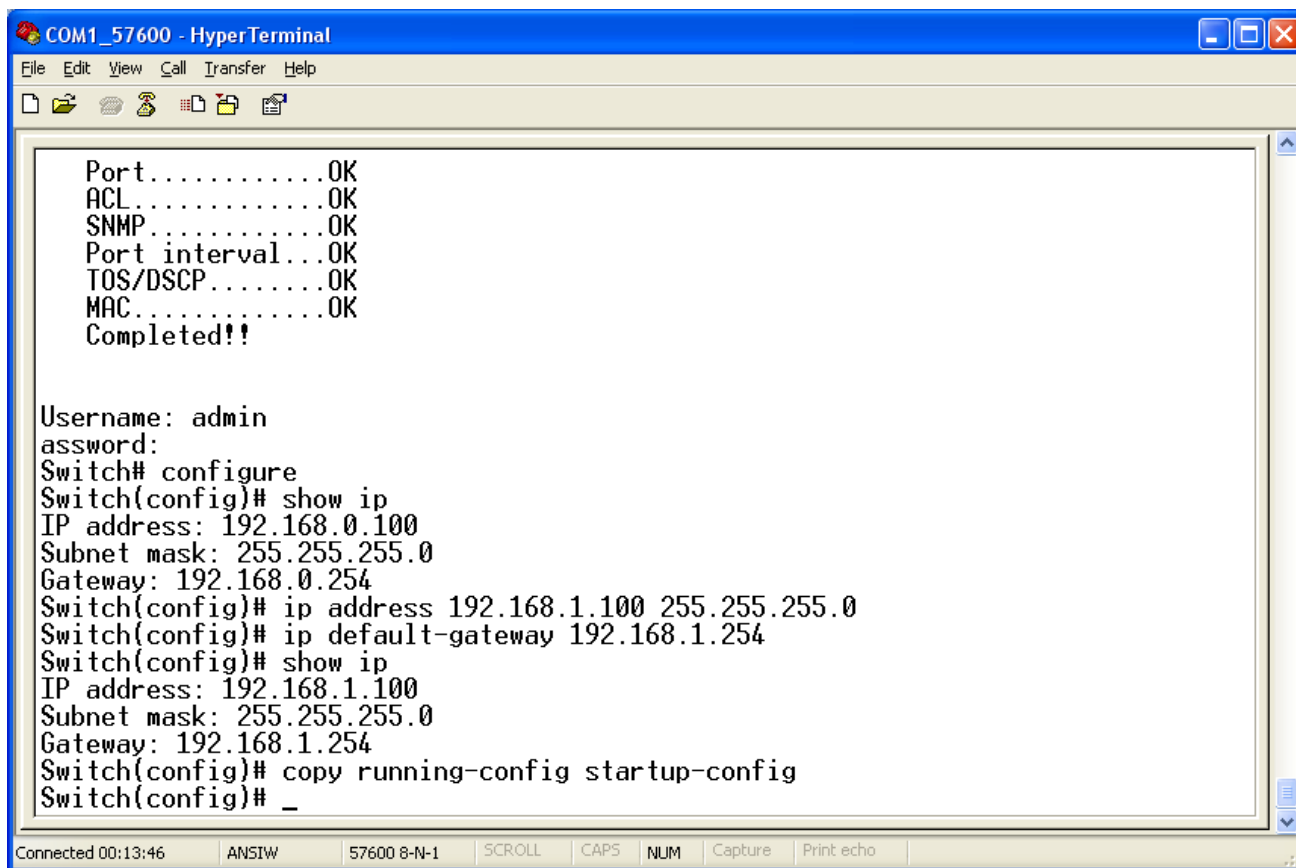
```
Switch(config)# ip address 192.168.1.100 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.254
```

The previous command would apply the follow settings for the Switch.

IP: 192.168.1.100

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254



```
COM1_57600 - HyperTerminal
File Edit View Call Transfer Help
Port.....OK
ACL.....OK
SNMP.....OK
Port interval...OK
TOS/DSCP.....OK
MAC.....OK
Completed!!

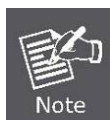
Username: admin
assword:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# ip address 192.168.1.100 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.254
Switch(config)# show ip
IP address: 192.168.1.100
Subnet mask: 255.255.255.0
Gateway: 192.168.1.254
Switch(config)# copy running-config startup-config
Switch(config)# _

Connected 00:13:46 ANSIW 57600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Figure 5-2-2: Set IP address screen

2. Repeat Step 1 to check if the IP address is changed.

If the IP is successfully configured, the Managed Switch will apply the new IP address setting immediately. You can access the Web interface of the Managed Switch through the new IP address.



If you do not familiar with console command or the related parameter, enter "**help**" anytime in console to get the help description.

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

5.3 Commands Level

The following table lists the CLI commands and description.

Modes	Access Method	Prompt	Exit Method	About This Mode ¹
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to: • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in User EXEC mode.	switch#	Enter disable to exit.	The privileged command is the advanced mode. Use this mode to • Display advanced function status • Save configuration
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure those parameters that are going to be applied to your switch.

6. COMMAND LINE INTERFACE

6.1 Operation Notice

To enter the “configuration” mode, you need to be in the privileged mode, and then types in the command **configure**:

```
Switch# configure
Switch (config) #
```

6.1.1. Command Line Editing

Keys Function

<Ctrl>-B	; ← Moves the cursor back one character.
<Ctrl>-D	Deletes the character at the cursor.
<Ctrl>-E	Jumps to the end of the current command line.
<Ctrl>-F	; → Moves the cursor forward one character.
<Ctrl>-K	Deletes from the cursor to the end of the command line.
<Ctrl>-N	; ↓ Enters the next command line in the command history.
<Ctrl>-P	; ↑ Enters the previous command line in the command history.
<Ctrl>-U	Deletes from the cursor to the beginning of the command line.
<Ctrl>	-W Deletes the last word typed.
<Esc> B	Moves the cursor backward one word.
<Esc> D	Deletes from the cursor to the end of the word.
<Esc> F	Moves the cursor forward one word.
<Backspace>	Delete the character before the cursor.
<Del>	Delete the character at the cursor.

The following generic function keys provide functions in all of the menus:

6.1.2. Command Help

You may enter ? at any command mode, and the CLI will return possible commands at that point, along with some description of each command

6.2 System Commands

show running-config

Description:

Display the running configuration of the switch.

copy running-config startup-config

Description:

Backup the switch configurations.

erase startup-config

Description:

Reset to default factory settings at next boot time.

clear arp

Description:

<ip-addr> specifies the IP address to be cleared. If no IP address is entered, the entire ARP cache is cleared.

show arp

Description:

Show the IP ARP translation table.

ping

Description:

Send ICMP ECHO_REQUEST to network hosts.

Parameters:

<1-999> specifies the number of repetitions. If not entered, it will continue to ping until you press <Ctrl>-C to stop.

6.3 Switch Static Configuration

6.3.1 Port Configuration and show status

port state

Turn the port state on or off.

Syntax:

port state <on | off> [<port-list>]

Parameters:

<port-list> specifies the ports to be turn on or off. If not entered, all ports are turn on or off.

port nego

Description:

Set port negotiation.

Syntax

port nego <force | auto | nway-force> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port speed

Description:

Set port speed (in mbps) and duplex.

Syntax:

port speed <10 | 100 | 1000> <full | half> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port flow

Description:

Enable or disable port flow control.

Syntax:

port flow <enable | disable> [<port-list>]

Parameters:

The <enable | disable> enables or disables flow control.

<port-list> specifies the ports to be set. If not entered, all ports are set.

port rate

Description:

Set port effective ingress or egress rate.

Syntax:

port rate <ingress | egress> <0-8000> [<port-list>]

Parameters:

<0-8000> specifies the ingress or egress rate <0-8000>

<port-list> specifies the ports to be set. If not entered, all ports are set.

port priority

Description:

Set port priority.

Syntax:

port priority <disable | 0-7> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

<0-7> set the port-based priority for specified port(s)

port jumboframe

Description:

Set port jumbo frame. When port jumbo frame is enable, the port forward jumbo frame packet

Syntax:

port jumboframe <enable | disable> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

show port status

Description:

Show port status, including port State, Link, Trunking, VLAN, Negotiation, Speed, Duplex, Flow control, Rate control ,Priority, Security, BSF control.

```
Switch(config)# show port status
```

```
-----
Port   1   Information
-----
```

```
State: on
```

```
Link: down
```

```
Trunking: none
```

```
VLAN: DEFAULT
```

```
Priority: disable
```

```
Security: off
```

Port	2	Information

State: on		
Link: down		
Trunking: none		
VLAN: DEFAULT		
Priority: disable		
Security: off		

Port	3	Information

State: on		
Link: down		
--More--		

show port statistics

Description:

Show port statistics, including TxGoodPkt, TxBadPkt, RxGoodPkt, RxBadPkt, TxAabort, Collision, and DropPkt.

Parameters:

<port-id> specifies the port to be shown.

Switch(config)# show port statistics		

Port	1	Information

TxGoodPkt: 0		
TxBadPkt: 0		
RxGoodPkt: 0		
RxBadPkt: 0		
TxAbort: 0		
Collision: 0		
DropPkt: 0		

Port	2	Information

TxGoodPkt: 0		
TxBadPkt: 0		
RxGoodPkt: 0		
RxBadPkt: 0		
TxAbort: 0		
Collision: 0		
DropPkt: 0		

Port	3	Information

--More--		

show port protection

Description:

Show protected port information.

Switch(config)# show port protection			
-----+-----+-----			
Port	Protected	Group	
-----+-----+-----			
1	off	1	
2	off	1	
3	off	1	
4	off	1	
5	off	1	
6	off	1	
7	off	1	
8	off	1	
9	off	1	
10	off	1	
Trk1	off	1	

6.4 Trunk Configuration

Trunk allows the switch to combine ports so that they function like a single high-speed link. It can be used to increase the bandwidth to some devices to provide a high-speed link. For example, trunk is useful when making connections between switches or connecting servers to the switch. Trunk can also provide a redundant link for fault tolerance. If one link in the trunk failed, the switch can balance the traffic among the remaining links.



1. The 10/100 Mbps port cannot be trunked with Gigabit port (Port 9 and Port 10 of VCO-8, or Port25 and Port26 of VCO-24).
2. All ports in the same trunk group will be treated as a single port. If a trunk group exists, the ports belonging to that trunk will be replaced by "TRUNK #" in the VLAN configuration screen. The following example configures Port 1~ Port 2 as "TRUNK 1."

6.4.1 Trunking Commands

show trunks

Description:

Show trunking information.

```
Switch(config)# show trunk
Group ID | LACP | Ports | LACP Active
-----+-----+-----+-----
1 | Yes | 1, 2 | 1, 2
```

trunk add

Description:

Add a new trunk group.

Syntax:

```
trunk add <trunk-id> <lacp | no-lacp> <port-list> <active-port-list>
```

Parameters:

<trunk-id> specifies the trunk group to be added.

<lacp | no-lacp> to specify the added trunk group to be LACP enabled

<port-list> specifies the ports to be set.

<active-port-list> specifies the ports to be set to LACP active.

no trunk

Description:

Delete an existing trunk group.

Syntax:

```
no trunk <trunk-id>
```

Parameters:

<trunk-id> specifies the trunk group to be deleted

6.4.2 LACP Command

[no] lacp

Description:

Enable/disable LACP.

lacp system-priority

Description:

Set LACP system priority.

Syntax:

lacp system-priority <1-65535>

Parameters:

<1-65535> specifies the LACP system priority.

no lacp system-priority

Description:

Set LACP system priority to the default value 32768.

show lacp status

Description:

Show LACP enable/disable status and system priority.

```
Switch(config)# show lacp status
LACP is enabled.
LACP system priority: 32768
```

show lacp

Description:

Show LACP information.

show lacp agg

Description:

Show LACP aggregator information.

Syntax:

show lacp agg <trunk-id>

Parameters:

<trunk-id> specifies the trunk group to be shown.

show lacp port**Description:**

Show LACP information by port.

Syntax:

show lacp port *<port-id>*

Parameters:

<port-id> specifies the port to be shown.



If VLAN group exist, all of the members of static trunk group must be in same VLAN group.

6.5 VLAN Configuration

6.5.1 Virtual LANs

A Virtual LAN (VLAN) is a logical network group that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN within a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically. A station can belong to more than one VLAN group. VLAN prevents users from accessing network resources of another on the same LAN, thus the users can not see the hard disks and printers of another user in the same building. VLAN can also increase the network performance by reducing the broadcast traffic and enhance the security of the network by isolating groups.

The Managed Switch supports two types of VLANs:

- **Port-based**
- **IEEE 802.1Q (tag) –based**

Only one of the two VLAN types can be enabled at one time.

Port-based VLANs are VLANs where the packet forwarding decision is made based on the destination MAC address and its associated port. You must define the outgoing ports allowed for each port when you use port-based VLANs. In port-based VLANs, the packets received from one port can only be sent to the ports which are configured to the same VLAN. As shown in the following figure, the switch administrator configured port 1~2 as VLAN 1 and port 3~4 as VLAN 2. The packets received from port 1 can only be forwarded to port 2. The packets received from port 2 can only be forwarded to port 1. That means the computer A can send packets to computer B, and vice versa. The same situation also occurred in VLAN 2. The computer C and D can communicate with each other. However, the computers in VLAN 1 can not see the computers in VLAN 2 since they belonged to different VLANs.

IEEE 802.1Q (tag) -based VLANs enable the Ethernet functionality to propagate tagged packets across the bridges and provides a uniform way for creating VLAN within a network then span across the network. For egress packet, you can choose to tag it or not with the associated VLAN ID of this port. For ingress packet, you can forward this packet to a specific port as long as it is also in the same VLAN group.

The 802.1Q VLAN works by using a tag added to the Ethernet packets. The tag contains a VLAN Identifier (VID) which belongs to a specific VLAN group. And ports can belong to more than one VLAN.

The difference between a port-based VLAN and a tag-based VLAN is that the tag-based VLAN truly divided the network into several logically connected LANs. Packets rambling around the switches can be forwarded more intelligently. In the figure shown below, by identifying the tag, broadcast packets coming from computer A in VLAN1 at sw1 can be forwarded directly to VLAN1.

However, the switch could not be so smart in the port-based VLAN mechanism. Broadcast packets will also be forwarded to port 4 of sw2. It means the port-based VLAN can not operate a logical VLAN group among switches.

The Managed Switch supports both Port-based VLAN and Tag-based (802.1Q) VLAN modes. The default configuration is

tag-based (802.1Q) VLAN. In the 802.1Q VLAN, initially, all ports on the switch belong to default VLAN, VID is 1.



You cannot delete the default VLAN group in 802.1Q VLAN mode.

6.5.2 VLAN Mode: Port-based

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

show vlan mode

Description:

Display the current VLAN mode.

vlan mode

Description:

Change VLAN mode.

Syntax:

vlan mode *<disabled | port-based | dot1q>*

Parameters:

<disabled | port-based | dot1q> specifies the VLAN mode.



Change the VLAN mode for every time, user have to restart the switch for valid value.

6.5.3 Advanced 802.1Q VLAN Configuration

Ingress filters configuration

When a packet was received on a port, you can govern the switch to drop it or not if it is an untagged packet. Furthermore, if the received packet is tagged but not belonging to the same VLAN group of the receiving port, you can also control the switch to forward or drop the packet. The example below configures the switch to drop the packets not belonging to the same VLAN group and forward the packets not containing VLAN tags.

VLAN Commands:

show vlan mode

Description:

Display the current VLAN mode.

vlan mode

Description:

Change VLAN mode.

Syntax:

vlan mode <disabled | port-based | dot1q>

Parameters:

<disabled | port-based | dot1q> specifies the VLAN mode.



Change the VLAN mode for every time, user have to restart the switch for valid value.

vlan add

Description:

Add or edit VLAN entry.

Syntax:

vlan add <1-4094> **NAME** <cpu-port | no-cpu-port> **LIST** [**LIST**]

Parameters:

<1-4094> specifies the VLAN ID or Group ID (if port based VLAN mode)

NAME specifies the VLAN group name.

<cpu-port | no-cpu-port> specifies the CPU port belong this VLAN group.

LIST specifies the ports to be set to VLAN members.

[**LIST**] specifies the ports to be set to tagged members. If not entered, all members set to untagged.

```
e.g.. switch(config)# vlan add 1 vlan1 cpu-port 1-4
```

This VLAN entry has four members (from port1 to port4, including CPU port) and all members are untagged.

no vlan**Description:**

Delete VLAN entry.

Syntax:

no vlan <1-4094>

Parameters:

<1-4094> specifies the VLAN ID or group ID (if port based VLAN).

e.g. no vlan 1

show vlan**Description:**

Show VLAN entry information.

Syntax:

show vlan [<1-4094>]

Parameters:

<1-4094> specifies the VLAN ID, null means all valid entries.

e.g.

```
Switch(config)# show vlan 1
VLAN                : 1
Type                 : Static
Creation Time (sec.): 43
CPU Port             : Yes

  Port | Member
-----+-----
  Port1 | Untagged
  Port2 | Untagged
  Port3 | Untagged
  Port4 | Untagged
  Port5 | Untagged
  Port6 | Untagged
  Port7 | Untagged
  Port8 | Untagged
  Port9 | Untagged
  Port10 | Untagged
  Trk1 | Untagged
```

show vlan static**Description:**

Show static VLAN entry information.

show vlan pvid**Description:**

Show port default VLAN ID.

Syntax:

show vlan pvid [LIST]

Parameters:

[LIST] specifies the ports to be showed. If not entered, all port's PVID will be showed.

e.g.

```
Switch(config)# show vlan pvid
Port | PVID
-----+-----
Port1 | 1
Port2 | 1
Port3 | 1
Port4 | 1
Port5 | 1
Port6 | 1
Port7 | 1
Port8 | 1
Port9 | 1
Port10 | 1
Trk1 | 1
```

vlan filter

Description:

Set ingress filter rules.

Syntax:

vlan filter <enable | disable> <enable | disable> LIST

Parameters:

The first <enable | disable> specifies the non-members packet will be forwarded or not. If set enable, forward only packets with VID matching this port's configured VID.

The second <enable | disable> specifies the untagged frame will be dropped or not. If set enable, drop untagged frame.

show vlan filter

Description:

Show VLAN filter setting.

Syntax:

show vlan filter [LIST]

Parameters:

[LIST] specifies the ports to be showed. If not entered, all ports' filter rules will be showed.

```
Switch(config)# show vlan filter
```

Port	Rule 1	Rule 2
Filter	(nonmbr)	(untag)
Port1	Drop	Forward
Port2	Drop	Forward
Port3	Drop	Forward
Port4	Drop	Forward
Port5	Drop	Forward
Port6	Drop	Forward
Port7	Drop	Forward
Port8	Drop	Forward
Port9	Drop	Forward
Port10	Drop	Forward
Trk1	Drop	Forward

6.6 Misc Configuration

[no] mac-age-time

Description:

Disable MAC address age-out or set MAC address age-out time.

Syntax:

no mac-age-time

mac-age-time <6-1572858>

Parameters:

<6-1572858> specifies the MAC address age-out time. The MAC age-out time must be divisible by 6. Type the number of seconds that an inactive MAC address remains in the switch's address table.

show mac-age-time

Description:

Show MAC address age-out time

broadcast

Description:

Set broadcast storm filter mode to off, 1/2, 1/4, 1/8, 1/16

Syntax:

broadcast mode <off | 1/2 | 1/4 | 1/8 | 1/16>

broadcast select

Description:

Select the Broadcast storm filter packet type:

- **Unicast/Multicast:** Flood unicast/multicast filter
- **Control Packets:** Control packets filter
- **IP multicast:** IP multicast packets filter
- **Broadcast Packets:** Broadcast Packets filter

Syntax:

broadcast select <unicast/Multicast | control | ip-multicast | broadcast>

collision-retry**Description:**

Collision-Retry setting

Syntax:

collision-retry <off | 16 | 32 | 48>

Parameters:

- <16 | 32 | 48> – In Half-Duplex, collision-retry maximum is 16 (or 32, 48) times and packet will be dropped if collisions still happen
- off – In Half-Duplex, if happen collision will retry forever (Default).

6.7 Administration Configuration

6.7.1 Change Username / Password

hostname**Description:**

Set switch name.

Syntax:

hostname <name-str>

Parameters:

- <name-str> specifies the switch name. If you would like to have spaces within the name, use quotes ("") around the name.

no hostname

Reset the switch name to factory default setting.

[no] password**Description:**

Set or remove username and password for manager or operator.

Syntax:

[no] **password** <manager | operator | all>

Parameters:

The manager username and password is also used by the web UI.

6.7.2 IP Configuration

User can configure the IP setting and fill in the new value.

ip address

Description:

Set IP address and subnet mask.

Syntax:

ip address <ip-addr> <ip-mask>

ip default-gateway

Description:

Set the default gateway IP address.

Syntax:

ip default-gateway <ip-addr>

show ip

Description:

Show IP address, subnet mask, and the default gateway.

show info

Description:

Show basic information, including system info, MAC address, and versions.

```
Switch(config)# show info
Model name: VCO-8
Description: 8-Port VDSL2 + 2G TP/SFP Combo Managed Switch
MAC address: 00:33:86:44:55:66
Firmware version: 1.08
CLI version: 1.07
802.1x: disabled
GVRP: disabled
LLDP: disabled
IGMP: enabled
LACP: enabled
```

dhcp**Description:**

Set switch as dhcp client, it can get IP from dhcp server.



If you set this command, the switch will reboot.

show dhcp**Description:**

show dhcp enable/disable.

6.7.3 Reboot switch**boot****Description:**

Reboot (warm-start) the switch.

6.7.4 Reset to Default**erase startup-config****Description:**

Reset configurations to default factory settings at next boot time.

6.7.5 TFTP Update Firmware**copy tftp firmware****Description:**

Download firmware from TFTP server.

Syntax:

copy tftp firmware <ip-addr> <remote-file>

Parameters:

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be downloaded from the TFTP server.

6.7.6 Restore Configuration File**copy tftp <running-config | flash>****Description:**

Retrieve configuration from the TFTP server. If the remote file is the text file of CLI commands, use the keyword `running-config`.

If the remote file is the configuration flash image of the switch instead, use the keyword `flash`.

Syntax:

```
copy tftp <running-config | flash> <ip-addr> <remote-file>
```

Parameters:

`<ip-addr>` specifies the IP address of the TFTP server.

`<remote-file>` specifies the file to be downloaded from the TFTP server.

6.7.7 Backup Configuration File

copy <running-config | flash> tftp

Description:

Send configuration to the TFTP server. If you want to save the configuration in a text file of CLI commands, use the keyword `running-config`. If you want to save the configuration flash image instead, use the keyword `flash`.

Syntax:

```
copy <running-config | flash> tftp <ip-addr> <remote-file>
```

Parameters:

`<ip-addr>` specifies the IP address of the TFTP server.

`<remote-file>` specifies the file to be read from the TFTP server.

6.8 MAC limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

User can configure the MAC limit setting and fill in the new value.

mac-limit

Description:

Enable MAC limit.

no mac-limit

Description:

Disable MAC limit.

mac-limit**Description:**

Set port MAC limit value, 0 to turn off MAC limit of port.

Syntax:

mac-limit <port-list> <1-64>

show mac-limit**Description:**

Show MAC limit information, including MAC limit enable/disable, per-port MAC limit setting.

6.9 Port Mirroring Configuration

Port monitoring is a feature to redirect the traffic occurred on every port to a designated monitoring port on the switch. With this feature, the network administrator can monitor and analyze the traffic on the entire LAN segment. In the Managed Switch, you can specify one port to be the monitored ports and any single port to be the monitoring port. You also can specify the direction of the traffic that you want to monitor. After properly configured, packets with the specified direction from the monitored ports are forwarded to the monitoring port.



The default Port Monitoring setting is disabled.

mirror-port**Description:**

Set port monitoring information. (RX only | TX only | both RX and TX)

Syntax:

mirror-port <rx | tx | both> <port-id> <port-list>

Parameters:

rx specifies monitoring receive only.

tx specifies monitoring transmit only.

both specifies monitoring both receive and transmit.

<port-id> specifies the analysis port ID. This port receives traffic from all monitored ports.

<port-list> specifies the monitored port list.

show mirror-port**Description:**

Show port monitoring information

6.10 Quality of Service

There are four transmission queues with different priorities in the Managed Switch: **Highest**, **SecHigh**, **SecLow** and **Lowest**. The Managed Switch will take packets from the four queues according to its QoS mode setting. If the QoS mode was set to "Disable", the Managed Switch will not perform QoS on its switched network. If the QoS mode was set to "High Empty Then Low", the Managed Switch will never exhaust packets from a queue until the queues with higher priorities are empty. If the QoS mode was set to "**weight ratio**", the Managed Switch will exhaust packets from the queues according to the ratio. The default value of QoS mode is "**weight 8:4:2:1**." That means the switch will first exhaust 8 packets from the queue with highest priority, and then exhaust 4 packets from the queue with second high priority, and so on.

When the switch received a packet, the switch has to decide which queue to put the received packet into. In the Managed Switch, it will put received packets into queues according to the settings of "802.1p Priority" and "Static Port Ingress Priority." When the received packet is an 802.1p tagged packet, the switch will put the packet into a queue according to the 802.1p Priority setting.

Otherwise, the switch will put the packet into a queue according the setting of Static Port Ingress Priority.

- **802.1p Priority:** the 802.1p packet has a priority tag in its packet header. The range of the priority is 7~0. The Managed Switch can specify the mapping between 802.1p priority and the four transmission queues. In the default setting, the packets with 802.1p priority 0~1 are put into the queue with lowest priority, the packets with 802.1p priority 2~3 are put into queue with second low priority, and so on.
- **Static Port Ingress Priority:** each port is assigned with one priority 7~0. The priority of the packet received from one port is set to the same priority of the receiving port. When the priority of the received packet was determined, the packet is treated as an 802.1p packet with that priority and will be put into a queue according to the 802.1p Priority setting.

6.10.1 QoS Configuration

QoS mode:

- **First Come First Service:** The sequence of packets sent is depending on arrive orders.
- **All High before Low:** The high priority packets sent before low priority packets.
- **WRR:** Weighted Round Robin. Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest : 4 second-high means that the switch sends 8 highest-priority packets before sending 4 second-high priority packets.
- **QoS level:** 0~7 priority level can map to highest, second-high, second-low, lowest queue.

Commands:

qos priority

Description:

Set 802.1p priority.

Syntax:

qos priority <first-come-first-service | all-high-before-low | weighted-round-robin>

Parameters:

[<highest-weight>][<sec-high-weight>][<sec-low-weight>] [<lowest-weight >]

e.g. qos priority weighted-round-robin 8,4,2,1

qos level

Description:

Set priority levels to highest, second-high, second-low and lowest.

Syntax:

qos level < highest | second-high | second-low | lowest > <level-list>

Parameters:

<level-list> specifies the priority levels to be high or low.

Level must be between 0 and 7.

e.g. qos level highest 7

e.g. qos level lowest 0

show qos

Description:

Show QoS configurations, including 802.1p priority, priority level.

e.g.

```
Switch(config)# show qos
QoS configurations:
QoS mode: weighted round robin
Highest weight: 8
Second High weight: 4
Second Low weight: 2
Lowest weight: 1
802.1p priority[0-7]:
Lowest   Lowest   SecLow   SecLow   SecHigh  SecHigh  Highest  Highest
```

6.10.2 Per-Port Priority

port priority

Description:

Set port priority.

Syntax:

port priority <disable | [0-7]> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

e.g. port priority disable 1-5

6.11 MAC Address Configuration

clear mac-address-table

Description:

Clear all dynamic MAC address table entries.

mac-address-table static

Description:

Set static unicast or multicast MAC address. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

Syntax:

mac-address-table static <mac-addr> <vlan-id> <port-id | port-list>

no mac-address-table static mac-addr

Description:

Delete static unicast or multicast MAC address table entries.

Syntax:

no mac-address-table static <mac-addr> <vlan-id>

show mac-address-table

Description:

Display MAC address table entries.

```
Switch(config)# show mac-address-table
```

MAC Address	VLAN	Type	Source
00:08:B6:00:06:90	1	Dynamic	9
00:40:63:00:65:30	1	Dynamic	Trk1
00:03:63:F7:80:7F	1	Dynamic	9

show mac-address table static

Description:

Display static MAC address table entries.

show mac-address-table multicast

Description:

Display multicast related MAC address table.

smac-address-table static**Description:**

Set static unicast or multicast MAC address in secondary MAC address table. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

Syntax:

smac-address-table static <mac-addr> <vlan-id> <port-id | port-list>

show smac-address-table**Description:**

Display secondary MAC address table entries.

show smac-address-table multicast**Description:**

Display multicast related secondary MAC address table.

[no] filter**Description:**

Set MAC address filter. The packets will be filtered if both of the destination MAC address and the VLAN tag match the filter entry. If the packet does not have a VLAN tag, then it matches an entry with VLAN ID 1.

Syntax:

[no] filter <mac-addr> <vlan-id>

show filter**Description:**

Display filter MAC address table.

6.12 STP/MSTP Commands

[no] spanning-tree

Description:

Enable or disable spanning-tree.

spanning-tree forward-delay

Description:

Set spanning tree forward delay of CIST, in seconds.

Syntax:

spanning-tree forward-delay <4-30>

Parameters:

<4-30> specifies the forward delay, in seconds. Default value is 15.



The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree hello-time

Description:

Set spanning tree hello time of CIST, in seconds.

Syntax:

spanning-tree hello-time <1-10>

Parameters:

<1-10> specifies the hello time, in seconds. Default value is 2.



The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree maximum-age

Description:

Set spanning tree maximum age of CIST, in seconds.

Syntax:

spanning-tree maximum-age <6-40>

Parameters:

<6-40> specifies the maximum age, in seconds. Default value is 20.



The parameters must enforce the following relationships:

$$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$$

spanning-tree priority

Description:

Set spanning tree bridge priority of CIST and all MSTIs.

Syntax:

spanning-tree priority <0-61440>

Parameters:

<0-61440> specifies the bridge priority. The value must be in steps of 4096. Default value is 32768.

show spanning-tree

Description:

Show spanning-tree information.

show spanning-tree port

Description:

Show spanning tree per port information.

Syntax:

show spanning-tree port [<port-list>]

Parameters:

<port-list> specifies the port to be shown. Null means all ports.

spanning-tree protocol-version

Description:

Change spanning tree protocol version of CIST.

Syntax:

spanning-tree protocol-version <stp | mstp>

Parameters:

stp specifies the original spanning tree protocol (STP, 802.1D).

mstp specifies the multiple spanning tree protocol (MSTP, 802.1s)

spanning-tree max-hops

Description:

Set spanning tree bridge maximum hops of CIST and all MSTIs.

Syntax:

spanning-tree max-hops <1-40>

Parameters:

<1-40> specifies the bridge maximum hops. Default value is **20**.

spanning-tree name**Description:**

Set spanning tree bridge name of CIST.

Syntax:

spanning-tree name [<name-string>]

Parameters:

<name-string> specifies the bridge name. Default name is null.

spanning-tree revision**Description:**

Set spanning tree bridge revision of CIST.

Syntax:

spanning-tree revision <0-65535>

Parameters:

<0-65535> specifies the bridge revision. Default value is 0.

spanning-tree port path-cost**Description:**

Set spanning tree port path cost of CIST.

Syntax:

spanning-tree port path-cost <1-200000000> [<port-list>]

Parameters:

<1-200000000> specifies port path cost.

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree port priority**Description:**

Set spanning tree port priority of CIST.

Syntax:

spanning-tree port priority <0-240> [<port-list>]

Parameters:

<0-240> specifies the port priority. The value must be in steps of 16.

<port-list> specifies the ports to be set. Null means all ports.

[no] spanning-tree port mcheck**Description:**

Force the port of CIST to transmit MST BPDUs. No format means not force the port of CIST to transmit MST BPDUs.

Syntax:

[no] spanning-tree port mcheck [<port-list>]

Parameters:

<port-list> specifies the ports to be set. Null means all ports.

[no] spanning-tree port edge-port**Description:**

Set the port of CIST to be edge connection. No format means set the port of CIST to be non-edge connection.

Syntax:

[no] spanning-tree port edge-port [<port-list>]

Parameters:

<port-list> specifies the ports to be set. Null means all ports.

[no] spanning-tree port non-stp**Description:**

Disable or enable spanning tree protocol on the CIST port.

Syntax:

[no] spanning-tree port non-stp [<port-list>]

Parameters:

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree port point-to-point-mac**Description:**

Set the port of CIST to be point to point connection.

Syntax:

spanning-tree port point-to-point-mac <auto | true | false> [<port-list>]

Parameters:

auto specifies point to point link auto connection.

true specifies point to point link true.

false specifies point to point link false.

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree mst**Description:**

Set spanning tree bridge priority of MSTI.

Syntax:

spanning-tree mst <0-15> priority <0-61440>

Parameters:

<0-15> specifies the MSTI instance ID.

<0-61440> specifies the MSTI bridge priority. The value must be in steps of 4096. Default value is 32768.

spanning-tree mst <0-15> vlan [<vlan-list>]**Description:**

Set MSTI to map VLAN list.

Syntax:

spanning-tree mst <0-15> vlan [<vlan-list>]

Parameters:

<0-15> specifies the MSTI instance ID.

<vlan-list> specifies the mapped VLAN list. Null means all VLANs.

spanning-tree mst <0-15> port path-cost <1-200000000> [<port-list>]**Description:**

Set spanning tree port path cost of MSTI.

Syntax:

spanning-tree mst <0-15> port path-cost <1-200000000> [<port-list>]

Parameters:

<1-200000000> specifies port path cost.

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree mst <0-15> port priority <0-240> [<port-list>]**Description:**

Set spanning tree port priority of MSTI.

Syntax:

spanning-tree mst <0-15> port priority <0-240> [<port-list>]

Parameters:

<0-240> specifies the port priority. The value must be in steps of 16.

<port-list> specifies the ports to be set. Null means all ports.

no spanning-tree mst**Description:**

Delete the specific MSTI.

Syntax:

no spanning-tree mst <0-15>

Parameters:

<0-15> specifies the MSTI instance ID.

show spanning-tree

Description:

Show spanning-tree information of CIST.

show spanning-tree port

Description:

Show spanning tree port information of CIST.

Syntax:

show spanning-tree port [<port-list>]

Parameters:

<port-list> specifies the port to be shown. Null means all ports.

show spanning-tree mst configuration

Description:

Show MST instance map.

Syntax:

show spanning-tree mst configuration

show spanning-tree mst <0-15>

Description:

Show MST instance information.

Syntax:

show spanning-tree mst <0-15>

Parameters:

<0-15> specifies the MSTI instance ID.

show spanning-tree mst <0-15> port <1-10>

Description:

Show specific port information of MST instance.

Syntax:

show spanning-tree mst <0-15> port <1-10>

Parameters:

<0-15> specifies the MSTI instance ID.

<1-10> specifies port number.

show vlan spanning-tree

Description:

Show per VLAN per port spanning tree status.

Syntax:

show vlan spanning-tree

6.13 SNMP

Any Network Management running the simple Network Management Protocol (SNMP) can be management the switch.

6.13.1 System Options

[no] snmp

Description:

Enable or disable SNMP.

show snmp status

Description:

Show the enable or disable status of SNMP.

snmp system-name

Description:

Set agent system name string.

Syntax:

snmp system-name <name-str>

Parameters:

<name-str> specifies the system name string.

e.g. snmp system-name SWITCH

snmp system-location

Description:

Set agent location string.

Syntax:

snmp system-location <location-str>

Parameters:

<location-str> specifies the location string.

e.g. snmp system-location office

snmp system-contact

Description:

Set agent system contact string.

Syntax:

snmp system-contact <contact-str>

Parameters:

<contact-str> specifies the contact string.

e.g. snmp system-contact abc@sina.com

show snmp system

Description:

Show SNMP system information.

6.13.2 Community Strings

snmp community

Description:

Set SNMP community string.

Syntax:

snmp community <read-sysinfo-only | read-all-only | read-write-all><community-str>

Parameters:

<community-str> specifies the community string.

e.g. snmp community read-all-only public

no snmp community

Description:

Delete SNMP community string.

Syntax:

no snmp community <community-str>

Parameters:

<community-str> specifies the community string.

e.g. no snmp community public

show snmp community

Description:

Show SNMP community strings.

6.13.3 Trap Managers

snmp trap

Description:

Set SNMP trap receiver IP address, community string, and port number.

Syntax:

snmp trap <ip-addr> [<community-str>] [<1..65535>]

Parameters:

<ip-addr> specifies the IP address.

<community-str> specifies the community string.

<1..65535> specifies the trap receiver port number. Default value is 162 if not specified.

e.g. snmp trap 192.168.200.1 public

no snmp trap**Description:**

Remove trap receiver IP address and port number.

Syntax:

no snmp trap <ip-addr> [<1..65535>]

Parameters:

<ip-addr> specifies the IP address.

<1..65535> specifies the trap receiver port number.

e.g. no snmp trap 192.168.200.1

show snmp trap**Description:**

Show all trap receivers.

6.14 IGMP

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite.

[no] igmp**Description:**

Enable/disable IGMP snooping.

Syntax:

[no] igmp

[no] igmp fastleave**Description:**

Enable/disable IGMP snooping fast leave. If enable, switch will fast delete member who send leave report, else wait one sec.

Syntax:

[no] igmp fastleave

[no] igmp querier

Description:

Enable/disable IGMP snooping querier.

Syntax:

[no] igmp querier

[no] igmp crossvlan

Description:

Enable/disable IGMP snooping Cross VLAN

Syntax:

[no] igmp crossvlan

show igmp

Description:

Show IGMP snooping information.

Syntax:

show igmp <status | router | groups | table>

Parameters:

status specifies IGMP snooping status and statistics information.

router specifies IGMP snooping router's IP address.

groups specifies IGMP snooping multicast group list.

table specifies IGMP snooping IP multicast table entries.

igmp clear_statistics

Description:

Clear IGMP snooping statistics counters.

6.15 802.1x Protocol

[no] dot1x

Description:

Enable or disable 802.1x.

Syntax:

[no] dot1x

radius-server host

Description:

Set radius server IP, port number, and accounting port number.

Syntax:

radius-server host <ip-addr> <1024..65535> <1024..65535>

Parameters:

<ip-addr> specifies server's IP address.

The first <1024..65535> specifies the server port number.

The second <1024..65535> specifies the accounting port number.

radius-server key

Description:

Set 802.1x shared key.

Syntax:

radius-server key <key-str>

Parameters:

<key-str> specifies shared key string.

radius-server nas

Description:

Set 802.1x NAS identifier.

Syntax:

radius-server nas <id-str>

Parameters:

<id-str> specifies NAS identifier string.

show radius-server

Description:

Show radius server information, including radius server IP, port number, accounting port number, NAS identifier,

dot1x timeout quiet-period

Description:

Set 802.1x quiet period. (default: 60 seconds)

Syntax:

dot1x timeout quiet-period <10-65535>

Parameters:

<10-65535> specifies the quiet period, in seconds.

dot1x timeout tx-period

Description:

Set 802.1x Tx period. (default: 15 seconds).

Syntax:

dot1x timeout tx-period <10-65535>

Parameters:

<10-65535> specifies the Tx period, in seconds.

dot1x timeout supplicant

Description:

Set 802.1x supplicant timeout (default: 30 seconds)

Syntax:

dot1x timeout supplicant <10-300>

Parameters:

<10-300> specifies the supplicant timeout, in seconds.

dot1x timeout radius-server

Description:

Set radius server timeout (default: 30 seconds).

Syntax:

dot1x timeout radius-server <10-300>

Parameters:

<10-300> specifies the radius server timeout, in seconds.

dot1x max-req

Description:

Set 802.1x maximum request retries (default: 2 times).

Syntax:

dot1x max-req <1-10>

Parameters:

<1-10> specifies the maximum request retries.

dot1x timeout re-authperiod

Description:

Set 802.1x re-auth period (default: 3600 seconds).

Syntax:

dot1x timeout re-authperiod <30-65535>

Parameters:

<30-65535> specifies the re-auth period, in seconds.

show dot1x

Description:

Show 802.1x information, quiet period, Tx period, supplicant timeout, server timeout, maximum requests, and re-auth period.

dot1x port

Description:

Set 802.1x per port information.

Syntax:

dot1x port <fu | fa | au | no> <port-list>

Parameters:

fu specifies forced unauthorized.

fa specifies forced authorized.

au specifies authorization.

no specifies disable authorization.

<port-list> specifies the ports to be set.

show dot1x port

Description:

Show 802.1x per port information.

Syntax:

show dot1x port <port-list>

Parameters:

<port-list> specifies the ports to be set.

6.16 Access Control List

Packets can be forwarded or dropped by ACL rules include IPv4 or non-IPv4. The Managed Switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on

6.16.1 IPv4 ACL commands

no acl

Description:

Delete an ACL group.

Syntax:

no acl <1-220>

Parameters:

<1-220> specifies the group ID.

e.g. no acl 1

no acl count

Description:

Reset the ACL group count.

Syntax:

no acl count <GroupId>

Parameters:

GroupId: <1-220> specifies the group ID.

show acl

Description:

Show ACL group information.

Syntax:

show acl [<1-220>]

Parameters:

<1-220> specifies the group ID, null means all valid groups.

e.g.

```
Switch(config)# show acl 1
Group Id : 1
-----
Action : Permit
Rules:
Vlan ID : Any
IP Fragement : Uncheck
Src IP Address : Any
Dst IP Address : Any
L4 Protocol : Any
```

```
Port ID : Any
Hit Octet Count : 165074
Hit Packet count : 472
```

acl add <1-220> <permit | deny> <0-4094> ipv4 <0-255>

Description:

Add ACL group for IPv4.

Syntax:

```
acl add <1-220> <permit | deny> <0-4094> ipv4 <0-255> A.B.C.D A.B.C.D A.B.C.D A.B.C.D (check|unCheck)
<0-65535> <0-10>
```

Parameters:

<1-220> specifies the group ID.

<permit | deny> specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN ID. 0 means don't care.

<0-255> specifies the IP protocol. 0 means don't care.

A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

A.B.C.D specifies the Destination IP Address. 0.0.0.0 means don't care.

A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

(check|unCheck) specifies the IP Fragment. check: Check IP fragment field; unCheck: Not check IP fragment field.

<0-65535> specifies the Destination port number if TCP or UDP. 0 means don't care.

<0-10> specifies the Port ID. 0 means don't care.

e.g.

```
Switch(config)# acl add 1 deny 1 ipv4 0 192.168.1.1 255.255.255.255 0.0.0.0 0.0.0.0 unCheck 0 0
```

This ACL rule will drop all packet from IP is 192.168.1.1 with VLAN ID=1 and IPv4.

acl add <1-220> qosvoip <0-4094>

Description:

Add ACL group for IPv4.

Syntax:

```
acl add <1-220> qosvoip <0-4094> <0-7> <0-1F> <0-1F> <0-FF> <0-FF> <0-FFFF> <0-FFFF> <0-FFFF> <0-FFFF>
```

Parameters:

<1-220> specifies the group ID.

<0-4094> specifies the VLAN ID. 0 means don't care.

<0-1F> specifies the port ID value.

<0-1F> specifies the port ID mask.

<0-FF> specifies the protocol value.

<0-FF> specifies the protocol mask.

<0-FFFF> specifies the source port value.

<0-FFFF> specifies the source port mask.

<0-FFFF> specifies the destination port value.

<0-FFFF> specifies the destination mask.

e.g. `acl add 1 qosvoip 1 7 1 1 0 0 0 0 0 0`

6.16.2 Non-IPv4 ACL commands

`no acl <1-220>` and `show acl <1-220>` commands are same as IPv4 ACL commands.

`acl add <1-220> <permit | deny> <0-4094> nonipv4 <0-65535>`

Description:

Add ACL group for non-IPv4.

Syntax:

`acl add <1-220> <permit | deny> <0-4094> nonipv4 <0-65535>`

Parameters:

<1-220> specifies the group ID.

<permit | deny> specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN ID. 0 means don't care.

<0-65535> specifies the Ether Type. 0 means don't care.

e.g. `acl add 1 deny 0 nonipv4 2054`. This ACL rule will drop all packets for ether type is 0x0806 and non-IPv4.

6.17 Binding

Let device that has specific IP address and MAC address can use network. We can set specific IP address, MAC address, VLAN ID and port ID to bind, and device can cross switch if all conditions match.

6.17.1 SIP/SMAC binding commands

[no] bind

Description:

Enable or disable binding function.

no bind <ID >

Description:

Delete Binding group.

Syntax:

no bind <1-220>

Parameters:

<1-220> specifies the group ID.

e.g. no bind 1

show bind

Description:

Show Binding group information.

Syntax:

show bind [<1-220>]

Parameters:

<1-220> specifies the group ID, null means all valid groups.

e.g. show bind 1

bind add

Description:

Add Binding group.

Syntax:

bind add <1-220> A:B:C:D:E:F <0-4094> A.B.C.D <1-10>

Parameters:

<1-220> specifies the group ID.

A.B.C.D specifies the MAC address.

<0-4094> specifies the VLAN ID. 0 means don't care.

A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

A.B.C.D specifies the IP Address.

<1-10> specifies the Port ID.

e.g.

```
Switch(config)# bind add 1 00:11:22:33:44:55 0 192.168.1.1 1
```

This Binding rule will permit all packet cross switch from device's IP is 192.168.1.1 and MAC is 00:11:22:33:44:55 and this device connect to switch port ID=1.

6.18 VDSL2 Commands

interface	Commands for VDSL interfaces
profiles	Commands for VDSL profiles

6.18.1 VDSL2 interface Commands

Interface xdsl

Description:

Commands for xdsl interfaces

Syntax:

Interface xdsl <show | set>

interface xdsl show oid

Description:

Show VDSL Logic MIB entry

Syntax:

interface xdsl show oid <portid> <oid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show roid

Description:

Show VDSL Real MIB entry

Syntax:

interface xdsl show roid <port id> <oid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show status

Description:

Show line status

Syntax:

interface xdsl show status <portid>

Parameters:

<1-8> or <1-24> port ID

```
Switch(config)# interface xdsl show status 1
```

Status (Basic) of Line 1: Showtime

	Value	Description
Actual Data Rate	100992	(US) Kb/s
Actual Data Rate	100992	(DS) Kb/s
SNR Margin	79	(US) 0.1dB
SNR Margin	251	(DS) 0.1dB
Firmware Version	10201	

Status (Advance) of Line 1:

	Upstream	Downstream	
Actual delay	5	5	ms
Actual INP	20	20	0.1 symbols
15M CV	0	0	
1Day CV	0	0	
Total CV	0	0	
15M FEC	0	0	
1Day FEC	728	0	
Total FEC	728	0	
Previous Data Rate	0	100992	Kbps
Attainable Rate	106023	169169	Kbps
Electrical Length	11	11	0.1dB
SNR Margin	NA	--	(US0,--) 0.1 dB
SNR Margin	80	251	(US1,DS1) 0.1 dB
SNR Margin	80	250	(US2,DS2) 0.1 dB
SNR Margin	78	251	(US3,DS3) 0.1 dB
SNR Margin	NA	NA	(US4,DS4) 0.1 dB
15M Elapsed time	488	488	secs
15M FECS	0	0	
15M ES	0	0	
15M SES	0	0	
15M LOSS	0	0	
15M UAS	0	0	
1Day Elapsed time	69788	69788	secs
1Day FECS	7	5	
1Day ES	0	5	
1Day SES	0	0	
1Day LOSS	0	0	
1Day UAS	0	0	
Total FECS	0	0	
Total ES	0	0	
Total SES	0	0	
Total LOSS	0	0	
Total UAS	0	0	

Switch(config)#

interface xdsl show pm_line_curr**Description:**

Show current counters of xdsl lines

Syntax:

interface xdsl show pm_line_curr <portid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show pm_ch_curr**Description:**

Show current counters of xdsl channels

Syntax:

interface xdsl show pm_ch_curr <portid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show invent**Description:**

Show inventory of xdsl lines

Syntax:

interface xdsl show invent <portid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show threshold**Description:**

Show threshold of xdsl lines

Syntax:

interface xdsl show threshold <portid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show table**Description:**

Show xdsl2 line table

Syntax:

nterface xdsl show table <line | lineband | channelstatus | scstatus | scstatussegment | pmlineinitcurr> <portid>

Parameters:

line, show xdsl2Line Table

lineband, show xdsl2LineBandTable

channelstatus, show xdsl2ChannelStatusTable

scstatus, show xdsl2SCStatusTable

scstatussegment, show xdsl2SCStatusSegmentTable

pmlineinitcurr, show PMLineInitCurrTable

<1-8> or <1-24> port ID

6.18.2 VDSL2 profile Commands

profile xdsl-line

Description:

Commands for xdsl-line

Syntax:

profile xdsl-line new <profile_name>

profile xdsl-line del <profile_name>

profile xdsl-line show

profile xdsl-line save

profile xdsl-line init

profile xdsl-line

profile xdsl-line new

Description:

Create a new xdsl profile

Syntax:

profile xdsl-line new <profile_name>

profile xdsl-line del

Description:

Delete xdsl profile

Syntax:

profile xdsl-line del <profile_name>

profile xdsl-line show

Description:

Show all profile names or show detail information of a specified profile

Syntax:

profile xdsl-line show <profile> <profile_name>

profile xdsl-line show <profile>

profile xdsl-line show <sprofile>

profile xdsl-line show profile

Description:

Show exist profile name

Syntax:

profile xdsl-line show

```
Switch(config)# profiles xdsl-line show profile
```

Exist VDSL Config Profile

=====

VDSL Config Profile Name: default

VDSL Config Profile Name: user1

VDSL Config Profile Name: user2

VDSL Config Profile Name: user3

VDSL Config Profile Name: user4

VDSL Config Profile Name: user5

VDSL Config Profile Name: user6

VDSL Config Profile Name: user7

VDSL Config Profile Name: user8

VDSL Config Profile Name: user9

VDSL Config Profile Name: user10

VDSL Config Profile Name: user11

VDSL Config Profile Name: user12

VDSL Config Profile Name: user13

VDSL Config Profile Name: user14

VDSL Config Profile Name: user15

VDSL Config Profile Name: user16

VDSL Config Profile Name: user17

VDSL Config Profile Name: user18

VDSL Config Profile Name: user19

VDSL Config Profile Name: user20

profile xdsl-line show sprofile

Description:

Show system support profile ID

Syntax:

profile xdsl-line show sprofile

Switch(config)# **profiles xdsl-line show sprofile**

Supported profile:

AnnexA_R_POTS_D-32_EU-32_30a
 AnnexA_R_POTS_D-32_EU-32_17a
 AnnexA_R_POTS_D-32_EU-32_12b
 AnnexA_R_POTS_D-32_EU-32_12a
 AnnexA_R_POTS_D-32_EU-32_8a
 AnnexA_R_POTS_D-32_EU-32_8b
 AnnexA_R_POTS_D-32_EU-32_8c
 AnnexA_R_POTS_D-32_EU-32_8d
 AnnexA_R_POTS_D-64_EU-64_30a_NUS0
 AnnexA_R_POTS_D-64_EU-64_17a
 AnnexB_B7-1_997-M1c-A-7
 AnnexB_B7-2_997-M1x-M-8
 AnnexB_B7-3_997-M1x-M
 AnnexB_B7-4_997-M2x-M-8
 AnnexB_B7-5_997-M2x-A
 AnnexB_B7-6_997-M2x-M
 AnnexB_B7-9_997E17-M2x-A
 AnnexB_B7-10_997E30-M2x-NUS0
 AnnexB_B8-1_998-M1x-A
 AnnexB_B8-2_998-M1x-B
 AnnexB_B8-4_998-M2x-A
 AnnexB_B8-5_998-M2x-M
 AnnexB_B8-6_998-M2x-B
 AnnexB_B8-8_998E17-M2x-NUS0
 AnnexB_B8-9_998E17-M2x-NUS0-M
 AnnexB_B8-10_998ADE17-M2x-NUS0-M
 AnnexB_B8-11_998ADE17-M2x-A
 AnnexB_B8-12_998ADE17-M2x-B
 AnnexB_B8-13_998E30-M2x-NUS0
 AnnexB_B8-14_998E30-M2x-NUS0-M
 AnnexB_B8-15_998ADE30-M2x-NUS0-M
 AnnexB_B8-16_998ADE30-M2x-NUS0-A
 AnnexC_POTS_25-138_b
 AnnexC_POTS_25-276_b
 AnnexC_TCM-ISDN

profile xdsl-line save

Description:

Save all profile configurations

Syntax:

profile xdsl-line save

profile xdsl-line init**Description:**

Initialize profile from savefile

Syntax:

profile xdsl-line init

profile xdsl-line set**Description:**

Set commands for xdsl profile.

profile xdsl-line set dsl-bandplan**Description:**

To enable a predefined set of PSD-mask, PSD-Level and sub carrier mask dependent on profile and bandplan selection for a VDSL config profile

Syntax:

profile xdsl-line set dsl-bandplan <profile_name> <value>

profile xdsl-line set fix-rate**Description:**

Specify the profile to use fixed rate in bit/s

Syntax:

profile xdsl-line set fix-rate <profile_name> <value>

profile xdsl-line set margin-target-snr-ds**Description:**

Signal Noise Ratio margin target downstream settings

Syntax:

profile xdsl-line set margin-target-snr-ds <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-target-snr-us**Description:**

Signal Noise Ratio margin target upstream settings

Syntax:

profile xdsl-line set margin-target-snr-us <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-max-snr-ds

Description:

Signal Noise Ratio margin max downstream settings

Syntax:

profile xdsl-line set margin-max-snr-ds <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-max-snr-us

Description:

Signal Noise Ratio margin max upstream settings

Syntax:

profile xdsl-line set margin-max-snr-us <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-min-snr-ds

Description:

Signal Noise Ratio margin min downstream settings

Syntax:

profile xdsl-line set margin-min-snr-ds <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-min-snr-us

Description:

Signal Noise Ratio margin min upstream settings

Syntax:

profile xdsl-line set margin-min-snr-us <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set rate-limit-max-ds-ch1

Description:

CH1 Maximum Data Rate on Downstream direction settings

Syntax:

```
profile xdsl-line set rate-limit-max-ds-ch1 <profile_name> <value-dec>
```

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-max-us-ch1

Description:

CH1 Maximum Data Rate on Upstream direction settings

Syntax:

```
profile xdsl-line set rate-limit-max-us-ch1 <profile_name> <value-dec>
```

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-max-ds-ch2

Description:

CH2 Maximum Data Rate on Downstream direction settings

Syntax:

```
profile xdsl-line set rate-limit-max-ds-ch2 <profile_name> <value-dec>
```

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-max-us-ch2

Description:

CH2 Maximum Data Rate on Upstream direction settings

Syntax:

```
profile xdsl-line set rate-limit-max-us-ch2 <profile_name> <value-dec>
```

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-min-ds-ch1

Description:

CH1 Minimum Data Rate on Downstream direction settings

Syntax:

```
profile xdsl-line set rate-limit-min-ds-ch1 <profile_name> <value-dec>
```

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-min-us-ch1**Description:**

CH1 Minimum Data Rate on Upstream direction settings

Syntax:

profile xdsl-line set rate-limit-min-us-ch1 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-min-ds-ch2**Description:**

CH2 Minimum Data Rate on Downstream direction settings

Syntax:

profile xdsl-line set rate-limit-min-ds-ch2 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-min-us-ch2**Description:**

CH2 Minimum Data Rate on Upstream direction settings

Syntax:

profile xdsl-line set rate-limit-min-us-ch2 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set max-delay-ds-ch1**Description:**

CH1 Maximum Interleave Delay on Downstream direction settings

Syntax:

profile xdsl-line set max-delay-ds-ch1 <profile_name> <value-dec>

Parameters:

<0-63> ms

profile xdsl-line set max-delay-us-ch1**Description:**

CH1 Maximum Interleave Delay on Upstream direction settings

Syntax:

profile xdsl-line set max-delay-us-ch1 <profile_name> <value-dec>

Parameters:

<0-63> ms

profile xdsl-line set inp-min-prot-ds-ch1

Description:

CH1 Downstream minimum impulse noise protection in 4.3125kHz(symbol) settings

Syntax:

profile xdsl-line set inp-min-prot-ds-ch1 <profile_name> <value-dec>

Parameters:

<1-18>

profile xdsl-line set inp-min-prot-us-ch1

Description:

CH1 Upstream minimum impulse noise protection in 4.3125kHz(symbol) settings

Syntax:

profile xdsl-line set inp-min-prot-us-ch1 <profile_name> <value-dec>

Parameters:

<1-18>

profile xdsl-line set inp-min-prot8-ds-ch1

Description:

CH1 Downstream minimum impulse noise protection in 8.625kHz settings

Syntax:

profile xdsl-line set inp-min-prot8-ds-ch1 <profile_name> <value-dec>

Parameters:

<1-17>

profile xdsl-line set inp-min-prot8-us-ch1

Description:

CH1 Upstream minimum impulse noise protection in 8.625kHz settings

Syntax:

profile xdsl-line set inp-min-prot8-us-ch1 <profile_name> <value-dec>

Parameters:

<1-17>

profile xdsl-line set max-delay-ds-ch2

Description:

CH2 Maximum Interleave Delay on Downstream direction settings

Syntax:

```
profile xdsl-line set max-delay-ds-ch2 <profile_name> <value-dec>
```

Parameters:

<0-63> ms

profile xdsl-line set max-delay-us-ch2

Description:

CH2 Maximum Interleave Delay on Upstream direction settings

Syntax:

```
profile xdsl-line set max-delay-us-ch2 <profile_name> <value-dec>
```

Parameters:

<0-63> ms

profile xdsl-line set inp-min-prot-ds-ch2

Description:

CH2 Downstream minimum impulse noise protection in 4.3125kHz(symbol) settings

Syntax:

```
profile xdsl-line set inp-min-prot-ds-ch2 <profile_name> <value-dec>
```

Parameters:

<1-18>

profile xdsl-line set inp-min-prot-us-ch2

Description:

CH2 Upstream minimum impulse noise protection in 4.3125kHz(symbol) settings

Syntax:

```
profile xdsl-line set inp-min-prot-us-ch2 <profile_name> <value-dec>
```

Parameters:

<1-18>

profile xdsl-line set inp-min-prot8-ds-ch2

Description:

CH2 Downstream minimum impulse noise protection in 8.625kHz settings

Syntax:

```
profile xdsl-line set inp-min-prot8-ds-ch2 <profile_name> <value-dec>
```

Parameters:

<1-17>

profile xdsl-line set inp-min-prot8-us-ch2

Description:

CH2 Upstream minimum impulse noise protection in 8.625kHz settings

Syntax:

```
profile xdsl-line set inp-min-prot8-us-ch2 <profile_name> <value-dec>
```

Parameters:

<1-17>

7. SWITCH OPERATION

7.1 Address Table

The Switch is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This information comes from the learning process of Ethernet Switch.

7.2 Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

7.3 Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

7.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters. Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

7.5 Auto-Negotiation

The STP ports on the Switch have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by

detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)

8. TROUBLESHOOTING

This chapter contains information to help you solve problems. If the Ethernet Switch is not functioning properly, make sure the Ethernet Switch was set up according to instructions in this manual.

■ The Link LED is not lit

Solution:

Check the cable connection and remove duplex mode of the Ethernet Switch

■ Some stations cannot talk to other stations located on the other port

Solution:

Please check the VLAN settings, trunk settings, or port enabled / disabled status.

■ Performance is bad

Solution:

Check the full duplex status of the Ethernet Switch. If the Ethernet Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ Why the Switch doesn't connect to the network

Solution:

1. Check the LNK/ACT LED on the switch
2. Try another port on the Switch
3. Make sure the cable is installed properly
4. Make sure the cable is the right type
5. Turn off the power. After a while, turn on power again

■ 100Base-TX port link LED is lit, but the traffic is irregular

Solution:

Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

■ Switch does not power up

Solution:

1. AC power cord not inserted or faulty
2. Check that the AC power cord is inserted correctly
3. Replace the power cord if the cord is inserted correctly; check that the AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power

■ **While IP Address be changed or forgotten admin password –**

To reset the IP address to the default IP Address “192.168.0.100” or reset the password to default value. Press the hardware **reset button** at the front panel about **10 seconds**. After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



APPENDIX A—RJ-45/-21 Pin Assignment

A.1 Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

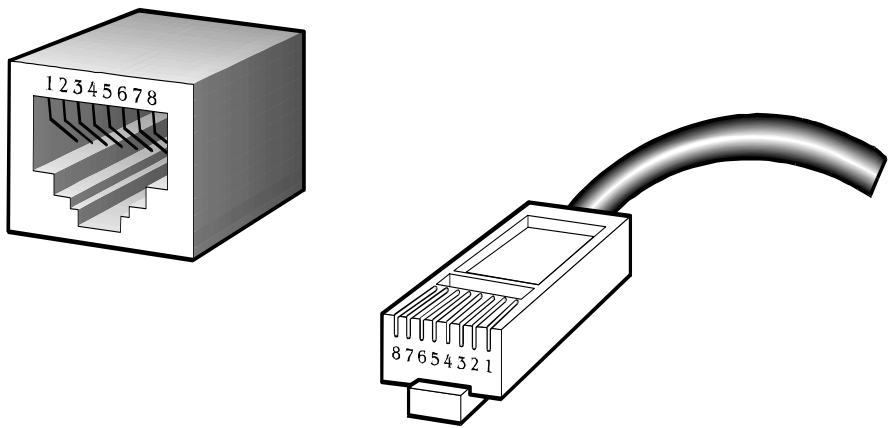
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	MDI Media Dependant Interface	MDI-X Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

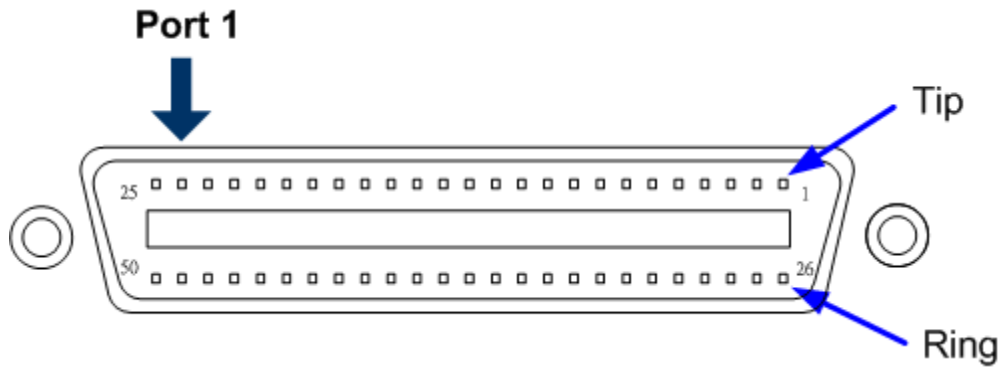
There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

Straight Cable			SIDE 1	SIDE 1	SIDE2			
1	2	3	4	5	6	7	8	
1	2	3	4	5	6	7	8	
			SIDE 2					
Crossover Cable			SIDE 1	SIDE 1	SIDE2			
1	2	3	4	5	6	7	8	
1	2	3	4	5	6	7	8	
			SIDE 2					

Figure A-1: Straight-Through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.

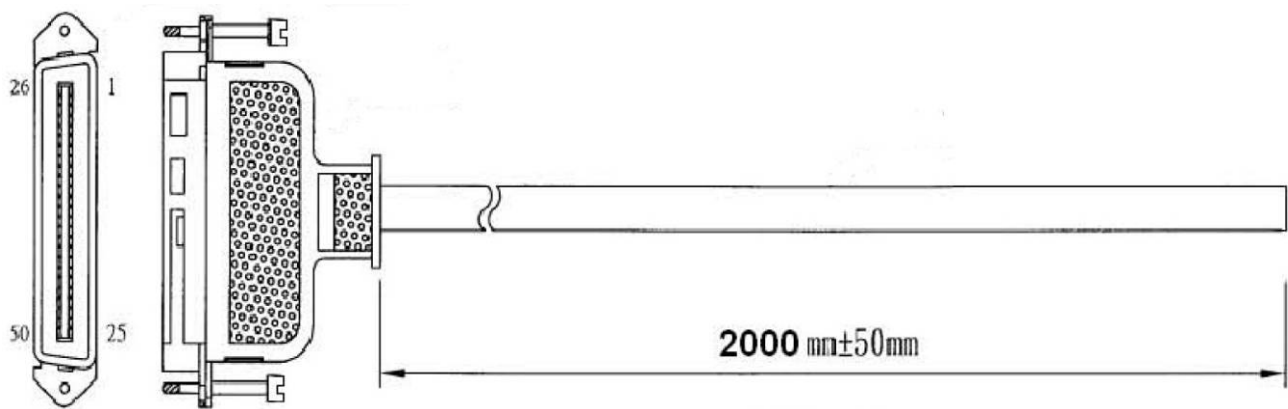
A.3 RJ-21 (Telco-50) Connector pin-out for VCO-24



The above picture is the RJ-21 connector on VCO-24 series. The following lists the RJ-21 connector pin outs:

Pin	Port / Function	Pin	Port / Function
1	Port 24, Tip	26	Port 24, Ring
2	Port 23, Tip	27	Port 23, Ring
3	Port 22, Tip	28	Port 22, Ring
4	Port 21, Tip	29	Port 21, Ring
5	Port 20, Tip	30	Port 20, Ring
6	Port 19, Tip	31	Port 19, Ring
7	Port 18, Tip	32	Port 18, Ring
8	Port 17, Tip	33	Port 17, Ring
9	Port 16, Tip	34	Port 16, Ring
10	Port 15, Tip	35	Port 15, Ring
11	Port 14, Tip	36	Port 14, Ring
12	Port 13, Tip	37	Port 13, Ring
13	Port 12, Tip	38	Port 12, Ring
14	Port 11, Tip	39	Port 11, Ring
15	Port 10, Tip	40	Port 10, Ring
16	Port 9, Tip	41	Port 9, Ring
17	Port 8, Tip	42	Port 8, Ring
18	Port 7, Tip	43	Port 7, Ring
19	Port 6, Tip	44	Port 6, Ring
20	Port 5, Tip	45	Port 5, Ring
21	Port 4, Tip	46	Port 4, Ring
22	Port 3, Tip	47	Port 3, Ring
23	Port 2, Tip	48	Port 2, Ring
24	Port 1, Tip	49	Port 1, Ring
25	No Connect	50	No Connect

A.4 RJ-21 (Telco 50) Cable pin-out



Port-24



Connector PIN	1	2	3	4	5	6	7	8	9
Wire Color	Blue	Orange	Green	Brown	Grey	Blue	Orange	Green	Brown
Connector PIN	26	27	28	29	30	31	32	33	34
Wire Color	White	White	White	White	White	Red	Red	Red	Red

Connector PIN	10	11	12	13	14	15	16	17	18
Wire Color	Grey	Blue	Orange	Green	Brown	Grey	Blue	Orange	Green
Connector PIN	35	36	37	38	39	40	41	42	43
Wire Color	Red	Black	Black	Black	Black	Black	Yellow	Yellow	Yellow

Connector PIN	19	20	21	22	23	24	25
Wire Color	Brown	Grey	Blue	Orange	Green	Brown	Grey
Connector PIN	44	45	46	47	48	49	50
Wire Color	Yellow	Yellow	Purple	Purple	Purple	Purple	Purple



Port-1